



# **SOUTH AFRICA**

# **CYBER THREAT INTELLIGENCE REPORT**

Weekly OSINT Brief, Week 38 | 6 September – 12 September 2026

**THREAT LEVEL: HIGH**

**TLP: CLEAR**

Report ID: SA-CTI-2026-W38 | Classification: TLP: CLEAR

**Published Monday 14 September 2026**

Compiled by Willem Steynberg – <https://www.linkedin.com/in/willem-steynberg-8a52234/>

Reviewed by Percy Kitso Sekate – <https://www.linkedin.com/in/percy-kitso-sekate/>

# TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W38)
- 4. Threat Actors
- 5. Critical Vulnerabilities & CISA KEV
- 6. Ransomware Landscape
- 7. OSINT Exposure & Attack Surface
- 8. Regulatory & Policy
- 9. Weekly Threat Hunt & IOCs
- 10. Strategic Recommendations
- 11. Threat Level Assessment
- 12. OSINT Sources Consulted



# TRAIN LIKE AN ATTACKER. LEVEL UP.

Live, virtual, instructor-led hacking courses — **attend online from anywhere.**

Two days per course · 09:00–17:00 (GMT+2) · Taught live by SensePost hackers



## 0xCD: Pragmatic API Exploration

Everything is an API: Learn to explore, test and exploit them.

**22–23 SEPT**  
2026



## 0xCD: Web Application Hacking

Sharpen your web app testing skills against real-world style targets.

**6–7 OCT**  
2026

- » Individual lab access for each person joining the training
- » Taught by ethical hackers with current field experience
- » Practical-driven learning through guided tasks, hands-on labs, and real-world style challenges
- » Content grounded in real methodologies and client work



### BOOK YOUR SEAT

**training+sept@orange cyberdefense.com**

**R20 500**  
PER COURSE



## 1. EXECUTIVE SUMMARY

### Overall Threat Level: HIGH, 21st consecutive week (6 September - 12 September 2026)

**Story 1.** Two ransomware operations listed two South African organisations twenty-two minutes apart on the evening of Sunday 7 September. The Gentlemen listed Hollard Insurance Group, the country's largest privately owned insurer with nearly four million policyholders and more than 4,000 staff, at 21:56 UTC; LockBit 5.0 listed VSB Attorneys, a conveyancing and commercial practice in Alberton, at 21:34 UTC.<sup>1,2,3,4</sup> Hollard told MyBroadband on 12 September that it is aware of the claims, has activated its incident response processes and cannot yet establish their validity, scope or impact; it has published nothing on its own site.<sup>3,5</sup> Neither listing carries a data volume, a sample or a deadline, and both are rated CLAIMED. First reported by [MyBroadband](#) on 12 September 2026.

**Story 2.** The confirmed material arrived through suppliers. On Saturday 12 September Bidvest Bank and EasyEquities each told customers that a third-party service provider had suffered a cyber incident and that customer data held there should be treated as potentially affected; neither named the provider, and EasyEquities described its provider as the firm that runs its client verification checks.<sup>6,7</sup> No source connects the two notifications and this report does not. Earlier in the week Cartrack confirmed to MyBroadband an incident that the publication reports as a ransomware attack, said systems have been restored and that it has notified the Information Regulator, which moves the DireWolf listing carried as CLAIMED in W37 to CONFIRMED for the incident; and Rohloff Group, the KFC franchisee listed by INC Ransom in W36, acknowledged the incident and said restaurant operations were not disrupted.<sup>8,9</sup> Four victim confirmations in one window is the most this series has carried, and two of the four concern someone else's breach.

**Story 3.** Fourteen vulnerabilities entered the CISA catalogue between 8 and 11 September, the largest weekly count this series has recorded, and seven were past their remediation date on Monday 14 September.<sup>10</sup> Seven sit on the network edge or the management plane: Citrix NetScaler, Cisco Secure Firewall Management Center at CVSS 10.0, FortiOS, two MikroTik RouterOS flaws, and the N-able N-central and ConnectWise ScreenConnect remote-management tools. Three of the vendor pages behind them would mislead a defender who read only the vendor: Fortinet's advisory still reads Known Exploited: No four days after the catalogue listing, Citrix's bulletin does not mention exploitation at all, and N-able's status page says no exploitation has been confirmed while its own customer notice says the opposite.<sup>11,12,13</sup> South Africa exposes 5,627 MikroTik RouterOS instances and 104 NetScaler instances to the internet, both VERIFIED counts.<sup>14</sup>

**W38 CORRECTION TO W37:** the W37 edition stated in three places that the Information Regulator's enforcement-notices register carried nothing later than 16 April 2025. That was wrong. The register's 2026 tab carries three instruments: Central Johannesburg TVET College dated 20 May 2026, Sibanye Stillwater dated 2 June 2026 and the Gauteng Department of Health notice dated 10 June 2026, which is the same instrument this report already used as the anchor for its weeks-since-publication count. The 16 April 2025 date was read from the 2025 tab alone. The KPI value of thirteen weeks in W37 was anchored on the June notice and stands; the W37 claim that the SABS notice is absent from the register also stands, since nothing dated August or September 2026 appears there. The corrections KPI row records one

correction this week.<sup>15,16</sup>

KPI Dashboard

| Metric                                                | Current (W38) | Prior (W37) | Change                | Direction |
|-------------------------------------------------------|---------------|-------------|-----------------------|-----------|
| Overall SA threat level                               | HIGH          | HIGH        | No change (21st week) | FLAT      |
| ransomware.live SA cumulative                         | 128           | 125         | +3                    | UP        |
| SA claims dated inside the window                     | 3             | 1           | +2                    | UP        |
| Window claims surviving the nationality check         | 2 of 3        | 1 of 1      | n/a                   | n/a       |
| SA breaches confirmed by the victim                   | 4             | 2           | +2                    | UP        |
| New CISA KEV additions                                | 14            | 10          | +4                    | UP        |
| KEV adds already overdue at publication               | 7             | 5           | +2                    | UP        |
| KEV adds with a published VERIFIED SA exposure figure | 6 of 14       | 1 of 10     | +5                    | UP        |
| Corrections issued to prior editions                  | 1             | 0           | +1                    | UP        |
| Weeks since last IR substantive publication           | 14            | 13          | +1                    | UP        |

Three notes on the table. The third ZA-tagged listing of the window, capricornlogistics.com, is an Indian company and is excluded from every South African count in this report; Section 3.6 sets out the check. The victim-confirmed row counts Cartrack, Rohloff Group, Bidvest Bank and EasyEquities, the last two confirming that their data sat in a breached supplier rather than that their own systems were entered. The exposure row counts six of fourteen catalogue entries with a published VERIFIED figure (MikroTik twice, NetScaler, FortiGate and Artifactory twice); a seventh figure, for ScreenConnect, was returned by the collection and is withheld for the reasons in Section 7.2.

**W38 KEY FRAMING:** the thing that failed this week belonged to someone else. Bidvest Bank and EasyEquities learned about their exposure from a provider; Cartrack's customers learned about theirs from a leak site before the company's statement reached the press; and a defender who checked the vendor page for Fortinet, Citrix or N-able on Friday 11 September would have read that exploitation was unconfirmed, unmentioned or denied while the CISA catalogue said otherwise for all three. A vendor's advisory records what the vendor has decided to say; the catalogue records what has been observed, and the two disagreed three times in one week. For a board the practical question is which of its suppliers, verification providers and software vendors would tell it first, and how many hours later. For a regulated financial institution the FSCA and Prudential Authority clock that started on 1 September runs from the moment the institution classifies an incident as material, and Saturday's two notifications are the first public test of what that looks like when the incident is a supplier's.

1. ransomware.live, victim record: Hollard Insurance Group, The Gentlemen, discovered 7 September 2026 21:56 UTC. <https://www.ransomware.live/id/SG9sbGFyZCBJbnNlcmFuY2UgR3JvdXBAdGhIZ2VudGxlbWVu>

2. ransomware.live, victim record: vsbattorneys.co.za, LockBit 5.0, discovered 7 September 2026 21:34 UTC.  
<https://www.ransomware.live/id/dnNiYXR0b3JuZXIzLmNvLnphQGxvY2tiaXQ1>
3. MyBroadband, South African insurance company allegedly hit by cyberattack (12 September 2026).  
<https://mybroadband.co.za/news/security/667199-south-african-insurance-company-allegedly-hit-by-cyberattack.html>
4. VSB Attorneys Inc, firm website, conveyancing and commercial practice at Meyersdal, Alberton, founded 1988, checked 13 September 2026. <https://www.vsbattorneys.co.za/>
5. Hollard, media centre press release index, most recent entry 26 August 2026, checked 13 September 2026.  
<https://www.hollard.co.za/media-centre/press-releases>
6. MyBroadband, South African bank notifies customers of data breach (12 September 2026).  
<https://mybroadband.co.za/news/security/667328-south-african-bank-notifies-customers-of-data-breach.html>
7. MyBroadband, EasyEquities informs customers about possible data breach (12 September 2026).  
<https://mybroadband.co.za/news/security/667348-easyequities-informs-customers-about-possible-data-breach.html>
8. MyBroadband, Top vehicle tracking company in South Africa with 2.2 million subscribers hit by cyberattack (7 September 2026). <https://mybroadband.co.za/news/security/666362-top-vehicle-tracking-company-in-south-africa-with-2-2-million-subscribers-hit-by-cyberattack.html>
9. MyBroadband, Large KFC franchise operator in South Africa hit by 536GB data breach (8 September 2026).  
<https://mybroadband.co.za/news/security/666413-large-kfc-franchise-operator-in-south-africa-hit-by-536gb-data-breach.html>
10. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.11, released 11 September 2026, retrieved 13 September 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
11. Fortinet PSIRT, FG-IR-25-084, heap-based buffer overflow in cw\_acd daemon, last updated 23 February 2026, still reading Known Exploited: No when checked 13 September 2026. <https://fortiguard.fortinet.com/psirt/FG-IR-25-084>
12. Citrix, NetScaler ADC and NetScaler Gateway security bulletin for CVE-2026-19489 and CVE-2026-19490, CTX696939 (19 August 2026, unrevised at 13 September 2026).  
<https://support.citrix.com/external/article/CTX696939/netscaler-adc-and-netscaler-gateway-secu.html>
13. Huntress, N-able N-central vulnerability exploitation (updated 6 September 2026).  
<https://www.huntress.com/blog/n-able-vulnerability-exploitation>
14. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 13 September 2026.  
<https://www.shodan.io/search?query=country%3AZA>
15. Information Regulator of South Africa, enforcement notices register; the 2026 tab carries three instruments dated 20 May, 2 June and 10 June 2026, checked 13 September 2026. <https://infoeregulator.org.za/enforcement-notice/>
16. Information Regulator of South Africa, Gauteng Department of Health enforcement notice dated 8 June 2026 and listed 10 June 2026, the anchor for the weeks-since-publication count.  
<https://infoeregulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>

## TOP 3 ACTIONS THIS WEEK

**1. Patch Citrix NetScaler on Monday 14 September, on both nodes of every HA pair, and check for sessions belonging to the user anonymous.** CVE-2026-19490 was due on 12 September and a public exploit was published before exploitation attempts began on 3 September. The fixed builds are 14.1-73.32 and 13.1-63.21; 12.1 and 13.0 are end of life with no fix. Bishop Fox confirmed the flaw on 13.1-63.18, so a 13.1 appliance below 13.1-63.21 is exposed regardless of earlier patching. On builds before 14.1-43.56 and 13.1-61.28 every Gateway and AAA virtual server is affected whether or not SAML is configured. South Africa exposes 104 NetScaler instances.

**2. Apply the Cisco FMC hot fix and run the vendor's log check, then patch MikroTik RouterOS and look for a user named ops.** CVE-2026-20079 is CVSS 10.0, unauthenticated, reaches root, and Cisco recorded active exploitation on 9 September; Talos ties one of three exploiting clusters to tradecraft consistent with Qilin affiliates. The check is one command in expert mode, `zgrep` for `package_info` and `license` across `/var/log/messages`, and a hit referencing `/var/tmp/license.tmp` means contact TAC rather than patch. VulnCheck's finding that exploitation needs a stale post-reboot session makes the FMC nobody logs into the most exploitable one. For RouterOS, 7.24.2, 7.23.4 or 6.49.21 closes the CERT Polska chain; a log line reading `user ops` added by `ssh:-2` is the published compromise marker.

**3. Write to every provider that verifies, onboards or screens your customers and ask two questions: whether it holds your data in an environment shared with other clients, and how many hours it will take to tell you.** EasyEquities' notification concerns a client verification provider and Bidvest Bank's concerns a provider holding limited categories of bank data; neither company can yet tell customers what was taken. Both wrote to customers before the forensic result was in, which is the right order. A regulated financial institution should also decide, this week and in writing, at what point a supplier's incident becomes material under Joint Communication 5 of 2026, because the 24-hour clock is measured from that classification.

## 2. THREAT LANDSCAPE HEATMAP

### South African Sector Threat Levels, Week 38 (6 September – 12 September 2026)



**Methodology:** each cell is an analyst score from 0 to 10 for the coming week, set from what this edition observed: leak-site listings with a South African tag that survives a nationality check, incidents confirmed by the organisation affected, catalogue additions affecting software the sector runs, VERIFIED South African exposure counts for that software, and reported fraud activity. It is a forward-looking prioritisation aid rather than a measurement, and a sector with no observation this week carries its prior score rather than dropping to zero.

**One row retired, one row added.** Telecommunications and VoIP is retired. Its score rose in W37 on the Sangoma Switchvox catalogue entry, nothing touching the sector was observed in this window, and the Switchvox entry stays in the Section 5 table where the overdue count belongs. Legal and Professional Services enters at 7 for ransomware, 7 for data extortion, 2 for hacktivism, 5 for phishing and fraud and 5 for vulnerability exploitation. It enters rather than rises. The basis is the LockBit 5.0 listing of VSB Attorneys, the fact that Professional Services is the joint most listed South African sector in the aggregator for 2026 at seven records alongside Financial Services, and the data class a conveyancing practice holds: identity documents, FICA packs and trust-account records for every property transaction it has handled.<sup>17,2</sup>

**Movements among the retained rows.** Financial Services and Credit rises from 5 to 7 on ransomware and from 6 to 8 on data extortion: an unresolved Gentlemen claim against the largest private insurer, and two institutions notifying customers of a supplier breach on the same day.<sup>1,6,7</sup> Its phishing and fraud score was already at the ceiling and stays there on SABRIC's 2025 figures, covered in Section 8. Transport, Logistics and Fleet rises from 6 to 7 on ransomware and from 7 to 8 on data extortion because the Cartrack listing became a confirmed ransomware incident with a regulator notification.<sup>8</sup> Network Edge and Remote Access rises from 6 to 7 on ransomware while holding 10 on vulnerability exploitation: Talos assesses one of the clusters exploiting Cisco FMC as a ransomware operator with tradecraft consistent with Qilin affiliates, and SOCRadar assesses the FortiOS campaign as Russian-speaking cybercrime, both against

products with VERIFIED South African exposure.<sup>18,19</sup> Government, Public Bodies and Defence holds; no initial access vector has been published for Rand Water and the hacktivism placeholder set in W37 stays until attribution arrives. Retail, Food and Consumer holds at 8 on data extortion with Rohloff's confirmation. Software Supply Chain and DevOps holds at the maximum with GitLab, two Artifactory entries and Adobe Commerce added. Collaboration and Virtualisation holds: the two Windows zero-days are local privilege escalations delivered through a browser chain, which is an endpoint problem rather than a collaboration-server one.

17. ransomware.live API, SA victim records, GET /v2/countryvictims/ZA, 128 records all tagged ZA, retrieved 02:00 UTC 13 September 2026. <https://api.ransomware.live/v2/countryvictims/ZA>

18. Cisco Talos, Ongoing exploitation of Cisco Secure Firewall Management Center (9 September 2026). <https://blog.talosintelligence.com/fmc-ongoing-exploitation/>

19. SOCRadar, CVE-2025-25249 exploited in the wild: PivotC2 RAT campaign against FortiGate (8 September 2026). <https://socradar.io/blog/cve-2025-25249-pivotc2-fortigate-rat/>

### 3. TOP SA INCIDENTS (W38)

Five incidents plus one exclusion. The order is by what a South African reader most needs to know rather than by evidence strength this week, because the two CLAIMED items involve the largest organisations and the three CONFIRMED items carry the actionable lesson. Every rating follows the standing rule that a leak-site description is written by the attacker and cannot lift a rating on its own.

#### 3.1 INC-2026-W38-01: Hollard Insurance Group, The Gentlemen Leak-Site Claim [CLAIMED]

|                   |                                                                                                                                                                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector            | Financial services and credit; short-term and life insurance                                                                                                                                                                                                                       |
| Organisation      | Hollard Insurance Group, <a href="https://hollard.co.za">hollard.co.za</a> , Johannesburg. Nearly four million policyholders, more than 10 million worldwide, more than 4,000 staff, turnover above R23 billion                                                                    |
| Actor and listing | The Gentlemen. Posted 7 September 2026, indexed 21:56 UTC, in a single-day batch alongside Air Canada, Los Angeles Metro and the University of San Francisco                                                                                                                       |
| Actor claim       | Sensitive data exfiltrated; full leak to follow unless the company makes contact. No data volume, file count, sample or deadline published                                                                                                                                         |
| Company response  | Statement to MyBroadband, 12 September: aware of the claims, incident response activated, internal teams and external specialists investigating, validity, scope and impact not yet established. No statement on Hollard's own site, whose newest press release is dated 26 August |
| Confidence        | CLAIMED. Actor assertion acknowledged by the company as under investigation; no confirmation of compromise, no regulator filing, no independent technical evidence                                                                                                                 |

The Gentlemen listed Hollard Insurance Group on 7 September 2026 with a profile-text description and no dataset, sample, size or deadline.<sup>1</sup> Hollard's statement to MyBroadband five days later confirms that the company is treating the matter as an incident and says nothing about whether an intrusion occurred; it explicitly declines to speculate while the investigation runs.<sup>3</sup> That is the correct posture and it leaves the rating where the evidence puts it. The one piece of context that favours taking the claim seriously is the

group's behaviour: The Gentlemen listed Babcock Africa on 19 August and has 838 victims on its leak site, with initial access in documented cases through infostealer-harvested credentials and unpatched FortiGate appliances, both of which are common in South African estates.<sup>20,21</sup> The piece that counsels caution is that the same group's Babcock listing has produced nothing in three and a half weeks. First reported by [MyBroadband](#) on 12 September 2026.

**Detection relevance:** TH-2026-W38-01 carries the group's kernel-driver EDR termination, GPO deployment and self-propagation behaviour with sourced indicators. For an insurer the pre-encryption signal to watch is the group's habit of enumerating VMware administrator groups and staging exfiltration with WinSCP or Rclone before anything is encrypted.

### 3.2 INC-2026-W38-02: Bidvest Bank and EasyEquities, Third-Party Provider Incidents [CONFIRMED]

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector        | Financial services and credit; banking and retail investment                                                                                                                                                                                                                                                                                                                                                                                                     |
| Organisations | Bidvest Bank; EasyEquities, a Purple Group business                                                                                                                                                                                                                                                                                                                                                                                                              |
| Disclosure    | Customer notifications reported by MyBroadband on Saturday 12 September 2026, in near-identical form                                                                                                                                                                                                                                                                                                                                                             |
| Confirmed     | Bidvest Bank: an unnamed service provider holding limited categories of bank data confirmed that the data sat in the affected environment and should be treated as potentially affected; own banking systems unaffected. EasyEquities: the unnamed third party that performs its client verification checks suffered a cybersecurity incident potentially affecting customer information; no evidence that EasyEquities or Purple Group systems were compromised |
| Not stated    | Which provider, what data categories, how many customers, whether the two providers are the same firm. Neither company mentions the Information Regulator or the FSCA in the reported text                                                                                                                                                                                                                                                                       |
| Confidence    | CONFIRMED for each company's own statement that its data was held in a breached supplier environment. Any connection between the two notifications is unproven and is not asserted                                                                                                                                                                                                                                                                               |

Bidvest Bank told customers that it does not yet know which clients may be affected and that it would rather say so now than wait for a complete picture; it warned that criminals use incidents like this to approach people while they are concerned, and that the bank will never ask for a PIN, password or OTP.<sup>6</sup> EasyEquities said the provider's forensic investigation had begun, that its own checks found no compromise of EasyEquities or Purple Group systems, and that customers contacted by anyone claiming to hold their data should not engage.<sup>7</sup> MyBroadband's second article notes the similarity of the two notices and stops there, which is also where this report stops: two financial institutions using unnamed verification or data providers notified customers on the same day, and whether that is one supplier or two is the observation next week will settle. First reported by [MyBroadband](#) on 12 September 2026.

Both companies wrote to customers before the supplier's investigation concluded, and both said plainly what they did not know. Set against The Courier Guy's denial in W35 and the twelve days it took a franchisee to acknowledge INC Ransom's listing, that is the disclosure practice the Information Regulator described at its 31 August briefing when it said a compromise should be reported once one is reasonably sure it occurred. **Detection relevance:** none in the institutions' own estates; the item belongs to supplier

assurance in Section 10, and to the materiality question in Section 8.2.

### 3.3 INC-2026-W38-03: Cartrack, Incident Confirmed and Regulator Notified [CONFIRMED]

|              |                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector       | Transport, logistics and fleet; vehicle telematics                                                                                                                                                                                                                                                                                                                                                    |
| Organisation | Cartrack, cartrack.co.za, wholly owned by Karooooo Limited; over 2.2 million subscribers at 31 May 2026                                                                                                                                                                                                                                                                                               |
| Disclosure   | Company statement dated 28 August, reported by MyBroadband on 7 September 2026, following DireWolf's leak-site listing of 2 September                                                                                                                                                                                                                                                                 |
| Confirmed    | An incident, which MyBroadband reports as a ransomware attack while Cartrack's quoted words say only the incident; steps taken to secure the environment; systems restored and platform operational; relevant authorities including the Information Regulator notified; affected parties to be notified once the data accessed is known. Picup unaffected; the event limited to Cartrack South Africa |
| Actor claim  | DireWolf claims 500 GB including financial documents, source code, customer profiles, NDAs and database backups, with sample folders posted, much of it relating to United States customers. The aggregator's victim page showed 100 GB in W37; both figures are the attacker's and neither is adopted                                                                                                |
| Confidence   | CONFIRMED for the incident and the regulator notification, on the company's own quoted statement. The ransomware characterisation is MyBroadband's. The volume and content of what was taken remain CLAIMED                                                                                                                                                                                           |

This closes the W37 watch item, and in the direction the item did not anticipate: Karooooo has filed no SENS announcement, whose index still ends on 28 July, and DireWolf has not published its full set, but the company answered a journalist.<sup>22,8</sup> Cartrack's statement confirms the incident, restoration, and notification of the Information Regulator, with the ransomware description being MyBroadband's rather than a quoted word of the company's, and it defers the section 22 notification of data subjects until the investigation says what was accessed. It also records that the Pick n Pay ASAP! outage of 2 September, which runs on Cartrack's Picup platform, was unrelated. First reported by [MyBroadband](#) on 7 September 2026.

Two observations for the record. The listing was CLAIMED in W37 with the note that a denial would not settle it; a confirmation does. DireWolf's tempo continues: the group's leak site was unreachable on 12 September and its listings have fallen 60 per cent month on month, so the 30-day publication practice noted in W37 may or may not run to schedule in early October.<sup>23</sup> **Detection relevance:** the DireWolf hunt ran as TH-2026-W37-01 and its indicators are unchanged; it is not repeated this week.

### 3.4 INC-2026-W38-04: VSB Attorneys, LockBit 5.0 Leak-Site Claim [CLAIMED]

|        |                                               |
|--------|-----------------------------------------------|
| Sector | Legal and professional services; conveyancing |
|--------|-----------------------------------------------|

|                          |                                                                                                                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organisation</b>      | VSB Attorneys Inc, vsbattorneys.co.za, Meyersdal, Albertyon, founded 1988. The firm's own site presents it as a conveyancing practice first, with corporate, estate and insolvency work alongside |
| <b>Actor and listing</b> | LockBit 5.0. Published 19:45 UTC, indexed 21:34 UTC, 7 September 2026. A leak screenshot is present; no data volume, ransom figure or deadline                                                    |
| <b>Actor claim</b>       | The listing text calls the firm a well-established practice specialising in corporate and commercial law, which paraphrases the firm's own site boilerplate; no data is described                 |
| <b>Corroboration</b>     | None. No firm statement, no Legal Practice Council comment, no South African media coverage located; two international breach trackers repeat the listing                                         |
| <b>Confidence</b>        | CLAIMED. Threat-actor assertion only                                                                                                                                                              |

LockBit 5.0 listed VSB Attorneys 22 minutes before The Gentlemen listed Hollard, and the two events are unrelated in every respect other than the calendar.<sup>2</sup> It is LockBit's first South African listing since Diesel-Electric on 1 March 2026 and its 24th in the aggregator's South African record, a history running back to 2021 that includes Nampak, the GPAA and several schools.<sup>17</sup> The firm's website is what it appears to be, a suburban conveyancing practice, and that is the reason the item is carried at this length despite its size: a conveyancer holds identity documents, FICA verification packs, bank details and trust-account records for every transfer it has handled, an exposure out of proportion to the firm's size.<sup>4</sup> No public statement exists from the firm and none was expected within the window; the Legal Practice Council has said nothing. **Detection relevance:** TH-2026-W38-07 carries the LockBit 5.0 encryptor's fixed behaviours and the aggregator's hash set for the group.

### 3.5 INC-2026-W38-05: Rohloff Group, INC Ransom Listing Acknowledged [CONFIRMED]

|                     |                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sector</b>       | Retail, food and consumer; quick-service restaurant franchising                                                                                                                                                                                                                                                                                                         |
| <b>Organisation</b> | Rohloff Group, Somerset West; 49 KFC outlets in South Africa and more than 100 across Africa; 1,000 to 5,000 employees                                                                                                                                                                                                                                                  |
| <b>Disclosure</b>   | Statement to MyBroadband, reported 8 September 2026, twelve days after the INC Ransom listing of 27 August recorded in the aggregator feed                                                                                                                                                                                                                              |
| <b>Confirmed</b>    | The company is aware of the cybersecurity incident affecting its systems; the incident has been contained; no disruption to restaurant operations (both direct quotes). MyBroadband further reports, in its own words, that required procedures were followed including regulatory and stakeholder notifications and that measures were taken to support those affected |
| <b>Actor claim</b>  | 536 GB, over 103,196 files across 30,805 folders, mostly employee data including bank statements, identity documents and disciplinary hearing results, plus royalty and food-cost records. Samples are published and contain employee and management personal information                                                                                               |
| <b>Confidence</b>   | CONFIRMED that an incident occurred and was contained, on the company's statement. The volume remains CLAIMED; the samples are actor-published and are not independently verified here                                                                                                                                                                                  |

Rohloff Group's statement upgrades an item carried as CLAIMED since W36 and answers the question W36 left open, which was whether anyone at the franchisee, KFC South Africa or Yum! Brands would say anything.<sup>9,17</sup> The reported reference to regulatory notifications does not name the Information Regulator, which is noted rather than read either way. The actor's published samples are reported to contain employee personal information, and the dataset described, bank statements, identity documents and disciplinary records for a workforce of that size, is the kind that produces secondary fraud against the individuals long after the corporate incident closes. First reported by [MyBroadband](#) on 8 September 2026. One statement in that coverage is contradicted by the local feed and is not carried: the aggregator records INC Ransom's Netstar listing in August 2025, not August 2026.<sup>17</sup> **Detection relevance:** INC Ransom's July SonicWall SMA 1000 chain remains the group's documented South African-relevant access route and is 59 days overdue in Section 5; no new INC indicators were published this week.

### 3.6 Not South African: capricornlogistics.com, Krybit

Krybit listed capricornlogistics.com on 12 September and the aggregator tagged the record ZA. The record's own description reads Capricorn Logistics Pvt. Ltd., an Indian supply chain company founded in 2001 in Mumbai, and the company's website carries a registered address in Andheri East, Mumbai, an Indian telephone number and a statistics block that counts Indian offices separately from overseas ones.<sup>24,25</sup> The country tag is an aggregator error, the third in this series after two Costa Rican companies in W33 and a Philippine one in W35, and the second to involve a transport company after Air Cote d'Ivoire. The record is excluded from every South African count in this report and the feed total of 128 is reported as the aggregator publishes it, with the derived count of two set beside it. One consequence follows for Section 4.3: Krybit's listing does not end its silence against South Africa.

### 3.7 Carryovers

- **Rand Water, W37.** No development in the window. No further SENS statement, no parliamentary question, no attribution and no statement about personal information could be located, and the parliamentary committee listing for 7 to 10 September carries nothing on it.<sup>26</sup> Rand Water's own media centre is client-side rendered and could not be read, so this is no publicly reported update rather than no update. Stays CONFIRMED for the intrusion; the three W37 tests remain open.
- **The Courier Guy, MedusaLocker, W35; Babcock Africa, The Gentlemen, W35; Furniture Bargaining Council, Deadlock, W36; Toyota South Africa's unnamed SMS provider, W34.** No development on any of them. All stay CLAIMED or open and are carried without re-argument.
- **Implats and Hungry Lion, W37.** No in-window development. The Implats article carries an undated post-publication update attributed to Anglo American Platinum rather than Implats, which cannot be placed in the window and is not used.

20. ransomware.live API PRO, group index GET /groups: The Gentlemen, 838 victims across 86 countries, retrieved 13 September 2026 (public page: ransomware.live/group/thegentlemen). <https://api-pro.ransomware.live/groups>

21. Blackpoint Cyber, Threat profile: The Gentlemen ransomware (3 August 2026). <https://blackpointcyber.com/threat-profile/gentlemen-ransomware/>

22. Karooooo Limited, JSE SENS announcements index, most recent entry 28 July 2026, checked 13 September 2026. <https://karooooo.com/jse-sens-announcements/>

23. ransomware.live API PRO, group index GET /groups: DireWolf, 135 victims across 37 countries, retrieved 13 September 2026 (public page: ransomware.live/group/direwolf). <https://api-pro.ransomware.live/groups>

24. ransomware.live, search API record: capricornlogistics.com, Krybit, discovered 12 September 2026, country field ZA against a description reading Indian, Mumbai. <https://api.ransomware.live/v2/searchvictims/capricorn>

25. Capricorn Logistics, company website, registered address Kondivita Road, Andheri East, Mumbai, telephone +91 22, checked 13 September 2026. <https://www.capricornlogistics.com/>

26. Parliamentary Monitoring Group, committee meetings index, complete listing for 7 to 10 September 2026, checked 13 September 2026. <https://pmg.org.za/committee-meetings/?page=1>

## 4. THREAT ACTORS

Three profiles. The Gentlemen and LockBit 5.0 each named a South African organisation inside the window. Krybit is closed as a watch item, with the reason.

### 4.1 The Gentlemen: Two South African Listings in Three Weeks

The Gentlemen emerged in mid-2025 from a split with Qilin: Blackpoint records that its operator, using the aliases hastalamuerte and zeta88, previously ran a Qilin affiliate and left over unpaid commissions, with the first sample on VirusTotal on 17 July 2025 and an affiliate programme on a 90/10 split.<sup>21</sup> It has grown faster than any comparable operation: Check Point counted 166 victims in the first quarter of 2026, a 315 per cent rise on the prior quarter and third globally, and the aggregator's group index carried 838 victims across 86 countries on 13 September, with Check Point placing it at 10 per cent of all published ransomware attacks in August behind Qilin at 15.<sup>27,20,28</sup> Its South African record is eight listings since January 2026, three of them municipalities, then Babcock on 19 August and Hollard on 7 September.<sup>17</sup>

Initial access is documented rather than guessed, which is unusual. Blackpoint names CVE-2024-55591 in FortiOS and FortiProxy as the primary vector and relays researcher reporting that the group maintains access to approximately 14,700 compromised FortiGate devices; Red Piranha and Surefire Cyber both record intrusions that began with employee credentials bought from infostealer markets.<sup>21,29</sup> Both routes are live in South Africa: FortiGate is the largest single appliance population in this report's exposure panel at 2,874, and the Hollard record itself carries third-party stealer-log telemetry of compromised employee credentials, which is an indicator of the access route the group prefers and is not evidence that it was used.<sup>14,1</sup>

On the host the tradecraft is distinctive. The group brings its own vulnerable driver, ThrottleStop.sys renamed ThrottleBlood.sys, loads it and exploits CVE-2025-7771 for kernel execution, then runs All.exe and Allpatch2.exe to terminate endpoint protection from the kernel; Allpatch2.exe identifies the running EDR dynamically rather than working from a fixed list. PowerRun.exe bypasses User Account Control for administrative rights, AnyDesk is installed as a service for persistence, PsExec and RDP with Restricted Admin mode enabled by setting DisableRestrictedAdmin to 0 handle lateral movement, reconnaissance scripts enumerate VMware administrator groups, and exfiltration goes out through WinSCP or Rclone.<sup>29,21</sup> Deployment is domain-wide through Group Policy via the NETLOGON share. Microsoft's May analysis adds the detail that matters most for containment: a spread argument turns the Go encryptor into a worm that attempts every reachable host using several lateral-movement methods at once, reusing the current session token when no credential is supplied; the note is README-GENTLEMEN.txt and Microsoft's sample appended .umc16h.<sup>30</sup> Blackpoint records lockers for Windows, Linux, BSD, NAS and ESXi, and Red Piranha's samples appended .7mtzh, so the six-character extension varies per build.<sup>21,29</sup> Encryption is Curve25519 with XChaCha20 per file, and Microsoft describes the operator-side decryptor; no public

decryptor exists.<sup>30</sup> The aggregator holds 85 sample hashes, 47 MD5, 34 SHA-256 and four SHA-1, and six Tox identifiers for the group; a representative subset is in iocs\_w38.csv.<sup>31</sup>

## 4.2 LockBit 5.0: Diversifying Away From the United States

LockBit resurfaced in September 2025 with a fifth version, nineteen months after Operation Cronos. Trend Micro's analysis of the Windows, Linux and ESXi builds establishes that it is a continuation of the family rather than an imitation, sharing hashing and API-resolution code with LockBit 4.0, and records the behaviours a defender can key on: a randomised 16-character extension, termination on Russian language settings or Russian geolocation, a patch to EtwEventWrite that disables event tracing, termination of security services matched against 63 hashed names, and a final pass through EvtClearLog to clear every event log. The ransom note is ReadMeForDecrypt.txt and the ESXi build targets virtual machine configuration files directly.<sup>32</sup> The group has 359 listed victims across 68 countries, its leak infrastructure was up 70.9 per cent of the time over the past 30 days, and it was last seen posting on 10 September.<sup>33</sup> Check Point's first-quarter figures record 163 victims, a 106 per cent rise, and a deliberate cut in United States concentration to 21.5 per cent after sustained law-enforcement pressure, which is the context in which a small South African law firm appears on the list.<sup>27</sup> No 2026 arrest, indictment or seizure against LockBit could be verified; Dmitry Khoroshev, indicted in May 2024, remains at large. The aggregator holds thirteen MD5 sample hashes for the LockBit 5.0 builds, a subset of which is in iocs\_w38.csv.<sup>31</sup>

## 4.3 Krybit: Watch Item Closed

W37 said this item would be retired after a fifth silent window, and this is that window as far as South Africa is concerned: the group's one ZA-tagged listing is an Indian company. The reading carried since W35, that the early-August burst of three South African listings in six days was one affiliate's scheduling, is consistent with a group whose only published research, SOCRadar's July profile, records seven panel users, a Babuk-derived encryptor, ransom demands of USD 40,000 to 100,000, no confirmed ransom payment and a victim list across 43 countries with no South African concentration mentioned at all.<sup>34</sup> Four South African listings in a year from a group with five affiliates is a run, and this report will treat the next one as a new observation rather than a resumption. Krybit's four MD5 hashes, two Tox identifiers and the .KRYBIT extension with RECOVER-README.txt remain in the aggregator's indicator feed for anyone who wants them.<sup>31</sup>

27. Industrial Cyber, reporting Check Point Research Q1 2026 ransomware figures: Qilin, LockBit and The Gentlemen expand influence (12 May 2026). <https://industrialcyber.co/ransomware/ransomware-sector-reconsolidating-as-qilin-lockbit-and-the-gentlemen-expand-influence-in-q1-2026/>

28. ITWeb, Check Point red flags heightened attacks on Africa's energy and utilities sectors (11 September 2026). <https://www.itweb.co.za/article/check-point-red-flags-heightened-attacks-on-africas-energy-and-utilities-sectors/Pero3MZ36XdqQb6m>

29. Red Piranha, The Gentlemen ransomware analysis (updated 11 June 2026). <https://redpiranha.net/news/the-gentlemen-ransomware-analysis>

30. Microsoft Threat Intelligence, The Gentlemen ransomware: dissecting a self-propagating Go encryptor (28 May 2026). <https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/>

31. ransomware.live API PRO, per-group endpoints GET /iocs/{group}, /yara/{group} and /ransomnotes/{group}, retrieved 13 September 2026 (key required; the public group pages carry the same sets). <https://api-pro.ransomware.live/iocs/thegentlemen>

32. Trend Micro, New LockBit 5.0 targets Windows, Linux, ESXi (25 September 2025). [https://www.trendmicro.com/es\\_mx/research/25/i/lockbit-5-targets-windows-linux-esxi.html](https://www.trendmicro.com/es_mx/research/25/i/lockbit-5-targets-windows-linux-esxi.html)

33. ransomware.live API PRO, group index GET /groups: LockBit 5.0, 359 victims across 68 countries, last seen 10 September 2026, retrieved 13 September 2026 (public page: ransomware.live/group/lockbit5). <https://api-pro.ransomware.live/groups>

34. SOCRadar, Dark web profile: Krybit ransomware (13 July 2026). <https://socradar.io/blog/dark-web-profile-krybit-ransomware/>

## 5. CRITICAL VULNERABILITIES & CISA KEV

Fourteen vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 8 and 11 September 2026, against ten the week before and the most in any window this series has recorded. Seven were past their remediation date on Monday 14 September, the day this report was published, and two more fell due on that day.<sup>10</sup> Every due date and overdue count in this section is arithmetic against the locally retrieved catalogue file, catalogVersion 2026.09.11, and every CVSS score is from the NVD feed with its scoring source recorded.<sup>10,35</sup> All fourteen carry knownRansomwareCampaignUse of Unknown, which is not the same as no. Nine of the fourteen received a three-day deadline under BOD 26-04, which is the catalogue's way of saying the exploitation evidence was strong at listing; those nine are the seven overdue items plus ScreenConnect and GitLab, which fell due on publication day.

**Citrix NetScaler CVE-2026-19490** is the entry with the clearest public exploit path. Citrix published the bulletin on 19 August, scoring it 9.3 under CVSS 4.0 as an authentication bypass on appliances configured as a Gateway or AAA virtual server, conditional on a SAML action only on the newer builds, and has not revised it since; the bulletin does not mention exploitation.<sup>12,35</sup> A proof of concept BleepingComputer describes as credible was published online and Previdian's sensors saw matching requests from 3 September, which BleepingComputer reported on 4 September alongside a Shadowserver count of more than 22,000 exposed NetScaler ADC and nearly 1,700 Gateway instances.<sup>36</sup> Bishop Fox's analysis of 10 September gives the defender the mechanics: the exploit is a POST to /cgi/samlauth in which the length of the decoded RelayState selects the code path, lengths 11 and 16 mint a session and lengths 18 and 21 crash the packet engine; every session created belongs to the user anonymous and appears as an SSL VPN login in clientless mode with an NSC\_AAAC cookie followed by /cgi/setclient?cvpn; an unpatched appliance answers the probe with HTTP 500 and internal error 43524 while a patched one answers 200 with Malformed Assertion; and the blast radius is gated by the default authorisation action, which ships as DENY and is commonly set to ALLOW in the field.<sup>37</sup> Two details change the patching decision. Bishop Fox obtained root command execution on 13.1-63.18, through a credentialed step it places outside the unauthenticated chain, so a 13.1 appliance below 13.1-63.21 is exposed whatever earlier NetScaler patching it received. And on builds before 14.1-43.56 and 13.1-61.28, every Gateway and AAA virtual server is affected whether or not SAML is configured. Fixed builds are 14.1-73.32, 13.1-63.21 and 13.1-37.277 for FIPS; Bishop Fox notes that 12.1 and 13.0 get no fix and must be migrated. South Africa exposes 104 instances.<sup>12,37,14</sup>

**Cisco Secure Firewall Management Center CVE-2026-20079** is the 10.0 of the set. Cisco first published the advisory on 4 March and revised it to version 2.5 on 9 September to record active exploitation, stating that its PSIRT became aware of it in August; the flaw lets an unauthenticated remote attacker bypass authentication and execute scripts as root on the underlying operating system, regardless of configuration, with no workaround.<sup>38</sup> Cisco's own indicator check is a single command in expert mode: `zgrep for package_info and license across /var/log/messages`, where a hit referencing `/var/tmp/license.tmp` indicates possible exploitation and the instruction is to contact TAC, because the hot fixes prevent future exploitation and may not remove an existing compromise.<sup>38</sup> Talos published three clusters on the same day. UAT-12197 uses the flaw alone to drop a JSP web shell in the Tomcat web root and steal credentials from the users table with `OmniQuery.pl`; UAT-11823, assessed with high confidence as an advanced persistent threat with tooling overlap to Sandworm, chains it with the July static-credential flaw CVE-2026-20316, exfiltrates the configurations of managed firewalls and deploys a Cyclops Blink implant; and UAT-11988, assessed with high confidence as a ransomware operator whose tradecraft is consistent

with Qilin affiliates, tunnels directory and remote-management ports through the appliance with SOCKS5 and reverse SSH before deploying Qilin.<sup>18</sup> VulnCheck, which built a working exploit in March and has kept it private, adds the condition that inverts the usual assumption: exploitation requires a stale post-reboot session that routine authenticated use of the console clears, so the FMC nobody logs into is the exploitable one, and any request carrying the static cookie CGISESSID=csm\_processes is exploit traffic.<sup>39</sup> No Shodan product label exists for this product and no South African figure is published.

**Fortinet CVE-2025-25249** is a heap overflow in the cw\_acd CAPWAP daemon of FortiOS and FortiSwitchManager, first published in January 2026 and listed now because SOCRadar published an in-the-wild campaign on 8 September: exploitation since at least July 2026 against more than 30,000 targeted addresses, 178 confirmed victim sessions of a remote access tool it names PivotC2, confirmed mailbox exfiltration from two United States organisations, and an assessment with high confidence of a Russian-speaking cybercrime campaign with no overlap with the FortiBleed operation attributed to INC and Lynx.<sup>19</sup> The attack surface is UDP 5246 wherever fabric appears in allowaccess, so firewalling the management interface does not cover it; fixed builds are 7.6.4, 7.4.9, 7.2.12 and 7.0.18, with 6.4 unfixed, and FortiSwitchManager 7.2.7 and 7.0.6, and the workaround is to remove fabric from allowaccess or deny UDP 5246 to 5249 with a local-in policy.<sup>11</sup> Two scoring facts are carried as found. The NVD feed gives 8.1 from the Fortinet PSIRT source, while the advisory page displays 7.4; and the advisory page, last updated 23 February 2026, still reads Known Exploited: No when read on 13 September, four days after the catalogue listing.<sup>35,11</sup> FortiGate is the largest population in this report's exposure panel at 2,874 South African instances, and that count is the product family rather than a count of unpatched builds.<sup>14</sup>

**MikroTik RouterOS CVE-2026-86060 and CVE-2026-67277** come from CERT Polska, which published six RouterOS vulnerabilities on 5 September after finding them with OpenAI's cyber-tuned models under an agentic research programme, with every hypothesis confirmed on real hardware. Two are in the catalogue: an argument injection in the SSH username that hands a session full administrator rights, scored 9.2, and a separate unauthenticated entry into the bandwidth-test service that leaks kernel memory or restarts the device, scored 8.8, both under CVSS 4.0.<sup>40,35</sup> The chain CERT Polska names MikroTrick pairs the argument injection with CVE-2026-67276, an SSH authentication bypass that is not itself in the catalogue; CERT Polska confirms that chain is being used to take full control of devices with internet-facing SSH, publishes the log lines login failure for user -2 and user added by ssh:-2, names the highly privileged account the attacker creates as ops, and records successful attacks from 82.192.72.4 since at least 2 September with attempts from 103.102.31.18.<sup>40</sup> MikroTik's notice of 3 September fixes the set in 7.25beta3, 7.24.2, 7.23.4 and 6.49.21, withholds detail deliberately, and notes RouterOS now marks a device Flagged when it finds selected compromise traces; CERT Polska warns that absence of the flag is not proof of safety.<sup>41,40</sup> This is the entry with the largest South African population in the panel: 5,627 RouterOS instances exposed, 4,584 of them on the API port 8728, a VERIFIED count promoted from the catalogue entry by the collection this week.<sup>14</sup> The country's wireless and fibre access networks run on this platform, so the figure is unsurprising and the exposure is real.

**N-able N-central CVE-2026-86218 and ConnectWise ScreenConnect CVE-2026-84869** are the remote-management pair. N-central's flaw is pre-authentication remote code execution on the server, scored 10.0 under CVSS 4.0 and fixed in 2026.3 Hotfix 4, build 2026.3.1.14, on 6 September; the status page says N-able has no confirmation of exploitation in production, while Huntress records that N-able's own customer notice called it exploited in the wild and reports a customer intrusion through a chain it describes as entirely distinct from the August flaws CVE-2026-18556 and CVE-2026-18577. Huntress ties its published tradecraft to the CVE-2026-86206 and CVE-2026-86207 authentication-bypass pair fixed in

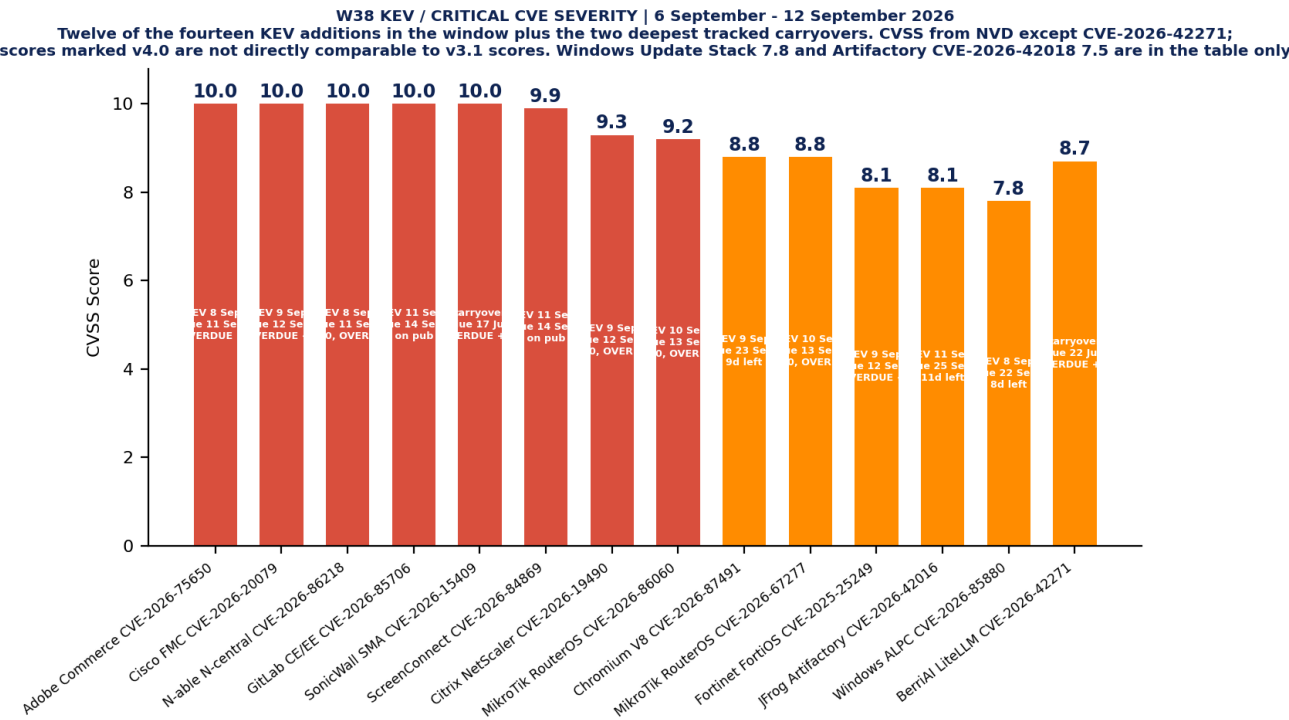
Hotfix 3, and says it cannot tell whether CVE-2026-86218 was the flaw used in that case: attacker addresses 23.234.100.105 and 23.234.97.68, accounts created by appending .invalid to known N-able addresses, and reconnaissance against /remoteControlAction.do.<sup>42,13,35</sup> ScreenConnect's flaw is on the client rather than the server: files can be transferred and executed through an active session without authorisation or host confirmation, scored 9.9, fixed in 26.6.5 on 8 September with cloud instances already upgraded and on-premise instances needing to be on 25.4 or later first; deselecting the TransferFiles permission per role is the interim control.<sup>43,35</sup> Huntress's three incidents from late August all began with social engineering, and the flaw is what turned each into worm-like spread: a backdoored client queued four VBScript files with the action set to Run at every technician machine that connected, delivering a wstunnel proxy, XMRig and a vulnerable WinRing0 driver.<sup>44</sup> The ScreenConnect exposure figure for South Africa is withheld, for the reasons in Section 7.2.

**Adobe Commerce CVE-2026-75650**, which Sansec calls StyleSmuggler, is an unauthenticated template-engine injection scored 10.0 that Adobe fixed on 7 September with a hotfix rather than a release; Adobe states it is aware of exploitation, and Sansec records the hotfix as the VULN-39341 composer patch together with Adobe's instruction to rotate the encryption key and every credential it protected.<sup>45,35,46</sup> Sansec first saw exploitation at 22:20 UTC on 4 September, three days before the patch, and found two unrelated operators on the same stores: one deploying a Rust implant that masquerades as kworker, fc-cache or chronyd and beacons over UDP 123 in NTP server mode, the other dropping a web shell under pub/media/catalog/product/cache that answers only to a fixed X-Cache-Token header.<sup>46</sup> Affected versions run from 2.4.4 to 2.4.9 for Commerce and 2.4.6 to 2.4.9 for Magento Open Source. **JFrog Artifactory CVE-2026-42016 and CVE-2026-42018** are a chain Wiz observed in use from 15 August to 8 September: an unauthenticated POST to /access/api/v1/aws/token/ returns an anonymous token when anonymous access is disabled, and a second request mints an administrator-scoped token from it, after which admin actions are logged as token:anonymous, actors create persistent accounts and install Groovy plugins for code execution; 59 per cent of organisations running Artifactory were still vulnerable six weeks after the first fix.<sup>47,48</sup> This is a third, separate Artifactory problem after CVE-2026-82329 and CVE-2026-66384, and the chain only reaches builds vulnerable to both. **GitLab CVE-2026-85706** is unauthenticated arbitrary file read through the repository commits API, scored 10.0 and fixed in 19.3.2, 19.2.6 and 19.1.8 on 10 September with database migrations that take a single-node instance down; watchTowr reproduced it, reports behavioural probes against its sensor network on 11 September, and gives a single hunt: POST requests to /api/v4/projects/{id}/repository/commits/ carrying a file.path parameter.<sup>49,50</sup> No confirmed compromise had been reported by anyone at the close of the window.

**The two Windows zero-days and the second Chrome zero-day** are one chain. Microsoft patched 964 vulnerabilities on 8 September, the most in any Patch Tuesday, with two exploited: CVE-2026-81963, a link-following elevation in the Windows Update Stack, and CVE-2026-85880, a heap overflow in ALPC, both 7.8 and both giving SYSTEM.<sup>51,35</sup> Google shipped Chrome 153.0.8010.36 the same day with CVE-2026-87491, an out-of-bounds write in V8 rated Medium by Google, stating that an exploit exists in the wild, five days after CVE-2026-85046.<sup>52</sup> Volatility and Proofpoint independently published the chain on 9 September: the earlier V8 flaw for code execution in the renderer, the new one for the sandbox escape, and the ALPC flaw for kernel privileges, in a kit Proofpoint calls BlueMoon, used by several espionage clusters, most with a suspected China nexus and some unattributed, against non-governmental organisations, aerospace and manufacturing; Proofpoint puts the earliest activity at 28 August and Volatility's own first observation is 1 September.<sup>53,54</sup> Two facts matter for a South African fleet. Proofpoint records that the fix for the first V8 flaw was committed to public Chromium source on 7 August and reached the stable channel on 3 September, a four-week window in which the attackers could read the diff;

and the kernel exploit rejects builds above 22000, which puts fully patched Windows 11 outside its reach and older Windows 10 and Server builds inside it.<sup>54,53</sup> The remedy is a browser restart and the September cumulative update; no hunt is written for the Windows Update Stack flaw because no exploitation detail has been published for it at all.

**Carryovers.** PaperCut shipped full security maintenance releases 26.0.5, 25.0.13 and 24.1.10 on 10 September, replacing all three emergency patches, with version 23 and earlier still unpatched.<sup>55</sup> GreyNoise and Blackpoint independently documented the campaign behind the exploitation: a likely Russian-speaking operator running hundreds of AI agents from 45.142.193.132 and 45.158.196.75 from 31 August, working from a recovered master list of 4,107 addresses of which 517 were passed into the campaign runner, compromising at least 440 instances at 395 organisations in 48 countries, harvesting credentials from 280 and reaching domain administrator at 12, with education the largest sector; the operator's own country exclusion list failed in places and South Africa appears in the victim table with nine instances.<sup>56,57</sup> Blackpoint's reading is the sober one: the AI reduced human effort across research, debugging and retries rather than producing a novel exploit. SonicWall SMA 1000 CVE-2026-83548 and CVE-2026-83549 are nine days overdue with no new material and an unrevised advisory; the July pair CVE-2026-15409 and CVE-2026-15410 are 59 days overdue with ransomware use recorded as Known; LiteLLM CVE-2026-42271 is 84 days overdue; SharePoint CVE-2026-55040 is 24 days overdue against 787 exposed South African instances.<sup>10,14</sup>



## W38 CISA KEV / Critical CVE Tracking (fourteen additions 8 to 11 September plus active carryovers)

| CVE            | Vendor / Product                             | CVSS       | Type                                 | KEV Due | Notes                                                                                                                                                                                                                                                                                                               |
|----------------|----------------------------------------------|------------|--------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-19490 | Citrix NetScaler ADC and Gateway             | 9.3 (v4.0) | Authentication bypass (unauth)       | 12 Sept | KEV 9 Sept. OVERDUE +2. Public PoC before exploitation attempts began 3 Sept. POST /cgi/samlauth; sessions as user anonymous. Root on 13.1-63.18 (Bishop Fox). Fixed 14.1-73.32 / 13.1-63.21 / 13.1-37.277 FIPS; 12.1 and 13.0 EOL. 104 in ZA. Ransomware: Unknown. EPSS 0.0560.                                    |
| CVE-2026-20079 | Cisco Secure FMC and SCC Firewall Management | 10.0       | Authentication bypass (unauth, root) | 12 Sept | KEV 9 Sept. OVERDUE +2. Cisco aware of exploitation since August; Talos clusters UAT-12197, UAT-11823 (Sandworm overlap) and UAT-11988 (Qilin-consistent). Check: zgrep package_info license /var/log/messages*. Hot fixes per branch; contact TAC on a hit. No ZA product label. Ransomware: Unknown. EPSS 0.7575. |
| CVE-2025-25249 | Fortinet FortiOS, FortiSwitchManager         | 8.1        | Heap overflow (CAPWAP, unauth)       | 12 Sept | KEV 9 Sept. OVERDUE +2. SOCRadar: PivotC2 RAT, 178 confirmed victim sessions, since July 2026. UDP 5246 where fabric in allowaccess. Fixed 7.6.4 / 7.4.9 / 7.2.12 / 7.0.18; 6.4 unfixed. Vendor page still says Known Exploited: No. FortiGate 2,874 in ZA. Ransomware: Unknown. EPSS 0.0240.                       |
| CVE-2026-86060 | MikroTik RouterOS                            | 9.2 (v4.0) | Argument injection (SSH username)    | 13 Sept | KEV 10 Sept. OVERDUE +1. CERT Polska: chained for full control; attacker creates user ops; log user added by ssh:-2; 82.192.72.4 active since 2 Sept. Fixed 7.24.2 / 7.23.4 / 6.49.21. 5,627 in ZA, 4,584 on API port 8728. Ransomware: Unknown. EPSS 0.0102.                                                       |

| CVE            | Vendor / Product                       | CVSS           | Type                                   | KEV Due | Notes                                                                                                                                                                                                                                                                                                                                             |
|----------------|----------------------------------------|----------------|----------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-67277 | MikroTik RouterOS                      | 8.8<br>(v4.0)  | Missing authentication (btest)         | 13 Sept | KEV 10 Sept. OVERDUE +1. Kernel memory disclosure or restart via the bandwidth-test service; a separate flaw from the MikroTrick chain, which pairs 86060 with the non-catalogue CVE-2026-67276. Same fixed builds. Ransomware: Unknown. EPSS 0.0086.                                                                                             |
| CVE-2026-86218 | N-able N-central                       | 10.0<br>(v4.0) | Static code injection (pre-auth RCE)   | 11 Sept | KEV 8 Sept. OVERDUE +3. Fixed 2026.3 Hotfix 4, build 2026.3.1.14. Vendor status page: no confirmed production exploitation; Huntress: net-new chain distinct from August; its IOCs (23.234.100.105, 23.234.97.68) belong to the 86206/86207 pair and it cannot say whether 86218 was used. No ZA product label. Ransomware: Unknown. EPSS 0.0074. |
| CVE-2026-75650 | Adobe Commerce and Magento Open Source | 10.0           | Template injection (unauth RCE)        | 11 Sept | KEV 8 Sept. OVERDUE +3. Exploited from 4 Sept, patched 7 Sept (composer hotfix VULN-39341 plus key rotation). Sansec: Rust implant with NTP-mimic C2 and a second operator's web shell. Commerce 2.4.4 to 2.4.9. No ZA product label. Ransomware: Unknown. EPSS 0.0215.                                                                           |
| CVE-2026-84869 | ConnectWise ScreenConnect              | 9.9            | Improper privilege management (client) | 14 Sept | KEV 11 Sept. Due on publication day. Fixed 26.6.5; cloud already upgraded; on-prem must be on 25.4 first. Huntress: worm-like VBS propagation after social-engineered install. ZA figure WITHHELD, see 7.2. Ransomware: Unknown. EPSS 0.0069.                                                                                                     |

| CVE            | Vendor / Product               | CVSS | Type                                      | KEV Due | Notes                                                                                                                                                                                                                                          |
|----------------|--------------------------------|------|-------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-85706 | GitLab CE and EE               | 10.0 | Path traversal (unauth file read)         | 14 Sept | KEV 11 Sept. Due on publication day. Fixed 19.3.2 / 19.2.6 / 19.1.8 with migrations. watchTower probes 11 Sept; hunt POST commits API with file.path. No confirmed compromise reported. No ZA product label. Ransomware: Unknown. EPSS 0.0115. |
| CVE-2026-81963 | Microsoft Windows Update Stack | 7.8  | Link following (local EoP)                | 22 Sept | KEV 8 Sept. Eight days to run. Patch Tuesday zero-day, exploited per Microsoft; no exploitation detail published by anyone. Client software. Ransomware: Unknown. EPSS 0.0063.                                                                 |
| CVE-2026-85880 | Microsoft Windows ALPC         | 7.8  | Heap overflow (local EoP)                 | 22 Sept | KEV 8 Sept. Eight days to run. Kernel stage of the BlueMoon chain (Volexity, Proofpoint); exploit rejects builds above 22000. Ransomware: Unknown. EPSS 0.0057.                                                                                |
| CVE-2026-87491 | Google Chromium V8             | 8.8  | Out-of-bounds write                       | 23 Sept | KEV 9 Sept. Nine days to run. Fixed 153.0.8010.36/.37; Google rates it Medium; sandbox-escape stage of BlueMoon. CVE-2026-85046 (due 18 Sept) is the renderer stage. Ransomware: Unknown. EPSS 0.0086.                                         |
| CVE-2026-42016 | JFrog Artifactory              | 8.1  | Incorrect authorisation (token scope)     | 25 Sept | KEV 11 Sept. Eleven days to run. Wiz chain observed 15 Aug to 8 Sept; admin actions log as token:anonymous. Fixed 7.133.11. 2 in ZA. Ransomware: Unknown. EPSS 0.0089.                                                                         |
| CVE-2026-42018 | JFrog Artifactory              | 7.5  | Improper authentication (anonymous token) | 25 Sept | KEV 11 Sept. Eleven days to run. POST /access/api/v1/aws/token/ returns a token with anonymous access disabled. Fixed 7.111.20 / 7.117.27 / 7.125.19 / 7.133.28 / 7.146.8. 2 in ZA. Ransomware: Unknown. EPSS 0.0092.                          |

| CVE            | Vendor / Product     | CVSS       | Type                                   | KEV Due | Notes                                                                                                                                                                                                                                                         |
|----------------|----------------------|------------|----------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-82078 | PaperCut NG/MF       | 9.4 (v4.0) | Unsafe reflection (Java bytecode exec) | 14 Sept | Carryover, due on publication day. Maintenance releases 26.0.5 / 25.0.13 / 24.1.10 on 10 Sept replace all emergency patches; CVE-2026-81578 shares the row. GreyNoise: AI-orchestrated campaign, 440 instances, nine in ZA. No ZA product label. EPSS 0.0169. |
| CVE-2026-83548 | SonicWall SMA 1000   | 10.0       | SSRF (unauth)                          | 5 Sept  | Carryover. OVERDUE +9. CVE-2026-83549 shares the dates. Advisory unrevised since 1 Sept; no IOCs, no attribution. Re-image where indicators found. No SMA-specific ZA figure. Ransomware: Unknown. EPSS 0.0467.                                               |
| CVE-2026-82329 | JFrog Artifactory    | 9.8        | Improper authentication (unauth admin) | 5 Sept  | Carryover. OVERDUE +9. Standalone, distinct from this week's chain. Kestra CVE-2026-49869 and Sangoma Switchvox CVE-2026-9586 share the 5 Sept due date and the +9. EPSS 0.0767.                                                                              |
| CVE-2026-55040 | Microsoft SharePoint | 9.1        | Weak authentication (JWT forgery)      | 21 Aug  | Carryover. OVERDUE +24. No new material this week; the September SharePoint update does not touch it. 787 in ZA. EPSS 0.5059, the highest among the carryovers.                                                                                               |
| CVE-2026-59822 | BerriAI LiteLLM      | 8.8 (v4.0) | Improper authentication (MCP)          | 16 Sept | Carryover. Two days to run. Starlette CVE-2026-48710 shares the date. Fixed 1.84.0, which also clears CVE-2026-42271 (due 22 Jun, OVERDUE +84, the deepest tracked). ZA figure WITHHELD, see 7.2. EPSS 0.0087.                                                |
| CVE-2026-15409 | SonicWall SMA 1000   | 10.0       | SSRF (unauth)                          | 17 Jul  | Carryover. OVERDUE +59. CVE-2026-15410 shares the dates and the KNOWN ransomware flag; INC Ransom affiliate and UTA0533 attributed in July. Rebuild rather than patch.                                                                                        |

**Pattern note: this week's set divides by whether the vendor's own page would tell you. For nine of the fourteen entries the exploitation evidence comes from a third party or from the catalogue alone, and the vendor page either omits it, contradicts it or predates it: Citrix's bulletin is silent, Fortinet's still reads Known Exploited: No, N-able's status page denies what its customer notice says, and the GitLab, Artifactory, MikroTik and ConnectWise pages carry the fix without the exploitation. For the other five the vendor says so itself: Adobe, Cisco, Google and Microsoft twice. The practical rule that follows is to read the catalogue first and the vendor page second, because the catalogue is the only place all fourteen appear with a date. On EPSS, Cisco FMC scores 0.7575 while NetScaler, with a public exploit and observed attempts, scores 0.0560 and MikroTik, with a named attacker address, scores 0.0102; EPSS predicts the next thirty days and lags confirmed activity, so it ranks items not yet in the catalogue and must never deprioritise one that is.<sup>58</sup> Two carryovers still outrank most of the additions: the July SonicWall pair at 59 days with ransomware use Known, and SharePoint at 24 days against 787 exposed South African instances with the highest EPSS of any carryover.<sup>10</sup>**

35. NVD API, CVSS base scores with scoring source, GET /rest/json/cves/2.0?cveId=, 53 CVEs resolved, retrieved 13 September 2026.  
<https://services.nvd.nist.gov/rest/json/cves/2.0>

36. BleepingComputer, Hackers target critical Citrix NetScaler auth bypass in attacks (4 September 2026).  
<https://www.bleepingcomputer.com/news/security/hackers-target-critical-citrix-netscaler-auth-bypass-in-attacks/>

37. Bishop Fox, Mind the config: detecting and weaponizing NetScaler CVE-2026-19490 (10 September 2026).  
<https://bishopfox.com/blog/mind-the-config-detecting-and-weaponizing-netscaler-cve-2026-19490>

38. Cisco, Security advisory cisco-sa-onprem-fmc-authbypass-5Jp45V2, version 2.5 updated to record active exploitation (9 September 2026).  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5Jp45V2>

39. VulnCheck, Cisco FMC authentication bypass CVE-2026-20079 analysis (26 March 2026).  
<https://www.vulncheck.com/blog/cisco-fmc-auth-bypass-cve-2026-20079>

40. CERT Polska, Vulnerabilities in MikroTik RouterOS actively exploited (5 September 2026).  
<https://cert.pl/en/posts/2026/09/vulnerabilities-in-mikrotik-routeros-actively-exploited/>

41. MikroTik, September 2026 vulnerability notice, fixed in RouterOS 7.24.2, 7.23.4 and 6.49.21 (3 September 2026).  
<https://mikrotik.com/supportsec/september-2026-vulnerability/>

42. N-able, N-central 2026.3 Hotfix 4 for CVE-2026-86218, build 2026.3.1.14 (6 September 2026).  
<https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/>

43. ConnectWise, ScreenConnect 26.6.5 security patch bulletin (8 September 2026).  
<https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin>

44. Huntress, Rogue ScreenConnect installations across unrelated hosts suggest worm-like activity (updated 9 September 2026).  
<https://www.huntress.com/blog/rogue-screenconnect-installations>

45. Adobe, Security update available for Adobe Commerce, APSB26-146 (7 September 2026).  
<https://helpx.adobe.com/security/products/magento/apsb26-146.html>

46. Sansec, StyleSmuggler: unauthenticated Magento zero-day exploited in the wild (5 September 2026, updated 11 September 2026).  
<https://sansec.io/research/stylesmuggler-0day>

47. Wiz Research, Artifactory under attack: in-the-wild exploitation of CVE-2026-42016 and CVE-2026-42018 (10 September 2026).  
<https://www.wiz.io/blog/artifactory-under-attack-in-the-wild-exploitation-of-cve-2026-42016-cve-2026-42018>

48. JFrog, Security advisories index, entries for CVE-2026-42016 (27 July 2026) and CVE-2026-42018 (12 August 2026).  
<https://docs.jfrog.com/releases/docs/jfrog-security-advisories>

49. GitLab, Critical patch release 19.3.2, 19.2.6 and 19.1.8 (10 September 2026).  
<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/>

50. watchTowr, Rapid reaction: GitLab critical path traversal CVE-2026-85706 (11 September 2026).  
<https://watchtowr.com/resources/rapid-reaction-gitlab-critical-path-traversal-vulnerability-cve-2026-85706/>

51. Tenable, Microsoft's September 2026 Patch Tuesday addresses 964 CVEs, CVE-2026-81963 and CVE-2026-85880 (8 September 2026).  
<https://www.tenable.com/blog/microsofts-september-2026-patch-tuesday-addresses-964-cves-cve-2026-81963-cve-2026-85880>

52. Google, Chrome Releases: stable channel update for desktop, 153.0.8010.36 and .37 (8 September 2026).  
[https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop\\_0808145027.html](https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html)

53. Volexity, Mind the patch gap: multiple Chinese threat actors chain zero-day exploits in Chrome and Windows (9 September 2026). <https://www.volexity.com/blog/2026/09/09/mind-the-patch-gap-multiple-chinese-threat-actors-chain-0-day-exploits-in-chrome-windows/>

54. Proofpoint, Once in a BlueMoon: multiple state-aligned threat actors rapidly adopt a novel exploit (9 September 2026). <https://www.proofpoint.com/us/blog/threat-insight/once-bluemoon-multiple-state-aligned-threat-actors-rapidly-adopt-novel-exploit>

55. PaperCut, Security bulletin of 27 August 2026, updated 10 September 2026 with security maintenance releases 26.0.5, 25.0.13 and 24.1.10. <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>

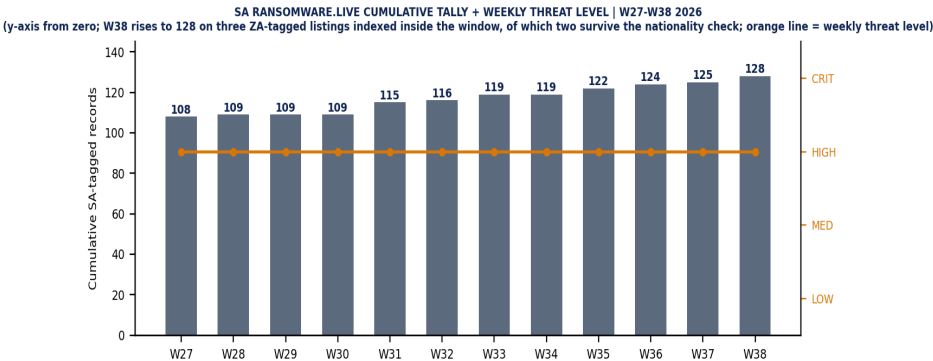
56. GreyNoise, Agents gone wild: an AI-orchestrated global campaign against PaperCut NG/MF (9 September 2026). <https://www.greynoise.io/blog/ai-orchestrated-campaign-against-papercut-ng-mf>

57. Blackpoint Cyber, Death by a thousand PaperCuts: AI-driven exploitation at scale (9 September 2026). <https://blackpointcyber.com/blog/death-by-a-thousand-papercuts-ai-driven-exploitation-at-scale/>

58. FIRST EPSS API, GET /data/v1/epss?cve=, 53 CVEs scored, retrieved 13 September 2026. <https://api.first.org/data/v1/epss>

## 6. RANSOMWARE LANDSCAPE

The South African victim feed held 128 records when retrieved at 02:00 UTC on 13 September 2026, up three on the previous week. The collection is country-scoped by path, the written file records 128 South African records against 128 returned, the run log records filter purity 1.0 and a clean exit, and the country filter that failed on 5 August is not in use.<sup>17</sup> A set-difference against the 6 September file returns three additions and zero removals: VSB Attorneys and Hollard Insurance Group on 7 September, and capricornlogistics.com on 12 September. Two of the three survive the nationality check; the third is Indian, as Section 3.6 sets out. The derived South African count for the window is therefore two, and the feed total of 128 is reported as the aggregator publishes it because adjusting it unilaterally would break comparability with the source.



|                                            |                                                                                                                                                                                                                                       |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Baseline at W37 close                      | 125 records                                                                                                                                                                                                                           |
| New listings dated inside the window       | 3 (vsbattorneys.co.za, LockBit 5.0, 7 September 21:34 UTC; Hollard Insurance Group, The Gentlemen, 7 September 21:56 UTC; capricornlogistics.com, Krybit, 12 September 10:31 UTC)                                                     |
| Delistings or restorations                 | None. Set difference against the 6 September file returns three additions and zero removals                                                                                                                                           |
| End count at W38 retrieval                 | 128 records, filter purity 1.0 in the run log and 128 of 128 tagged ZA in the file                                                                                                                                                    |
| Nationality check                          | 2 of 3 surviving. Capricorn Logistics is a Mumbai company; the ZA tag is an aggregator error                                                                                                                                          |
| Groups active against SA, rolling 120 days | 15 by discovery date, against 14 last week: LockBit 5.0 enters on the VSB listing. The rolling boundary moves each week, so this figure is not a trend                                                                                |
| Threat-level drivers                       | Two unresolved claims from two of the three most active operations in the world, four victim confirmations of which two are supplier breaches, and seven overdue catalogue additions across the network edge and the management plane |

Group notes. The Gentlemen and LockBit 5.0 are profiled in Section 4; between them and Qilin they accounted for a quarter or more of all published ransomware attacks in August, on Check Point's count of 1,042, almost double August 2025.<sup>28</sup> DireWolf's Cartrack listing is now a confirmed incident. INC Ransom's Rohloff listing is now an acknowledged one. Krybit's item is closed. Of the last ten ZA-tagged listings in the feed, two are not South African, and of the remaining eight, three have been confirmed by the organisation named: Cartrack, Rohloff Group and the Furniture Bargaining Council, with the last confirming encryption only.<sup>17</sup>

One measurement caution carried from prior editions and still binding. The victim feed is the free v2 tier and is delayed relative to the paid tier, so a listing dated inside this window may have been posted earlier, and one posted late on Saturday 12 September may not appear until next week's collection. The window closes at the end of Saturday because an earlier edition ran to Sunday midnight and missed two South African victims in the unobserved hours.

## 7. OSINT EXPOSURE & ATTACK SURFACE

### 7.1 What the Panel Publishes, and What It Cannot

Every figure in this section is an exposure count: how many instances of a product Shodan sees on the South African internet, not a count of vulnerable systems. The vuln: filter is unavailable on this collection's plan, so no figure here should be read as the number of South African systems affected by a given CVE. Only results the collection marks VERIFIED are published, which means the product facet corroborates the query rather than that anyone has confirmed a version. Two standing queries remain unpublishable, the Palo Alto GlobalProtect title match and the Arista VeloCloud zero, and four of this week's catalogue products were held for manual fingerprinting because Shodan has no product label for them: GitLab, Adobe Commerce, N-central and Chromium. Cisco FMC has never had one.<sup>14</sup> No organisation is named anywhere in this section.

## 7.2 Two Figures Withheld, and the Test That Separates Them

---

W37 withheld a count of 4,041 LiteLLM instances and set two tests: a re-derivation by a structured method, and stability across two collections. This week's collection returned 5,171, a rise of 28 per cent, which is neither the few per cent that would mark a stable population nor the order of magnitude that would settle it as an artefact; and the collection auto-promoted a second query from the ScreenConnect catalogue entry that returned 2,996 South African instances with a product facet 100 per cent on that family, so it too self-marked VERIFIED and publishable.<sup>14</sup> Neither is published, and this time there is a structured reason rather than an argument from plausibility.

The port distribution is the test. A real product population clusters on the ports the product listens on: of 2,874 FortiGate instances, 1,493 sit on 10443 and 705 on 541; of 924 Tomcat instances, 273 sit on 8080; of 5,627 MikroTik instances, 4,584 sit on the API port 8728. For LiteLLM the five most common ports carry nine, seven, six, six and six hosts, and for ScreenConnect the five most common carry four hosts each, none of them the product's defaults, which means thousands of hosts spread across hundreds of ports at a handful apiece.<sup>14</sup> That is the signature of a fingerprint matching something other than the product, or of a deception network answering with the product's banner on every port, and either way it is not a count of LiteLLM proxies or ScreenConnect clients. The ScreenConnect figure would also put 12.9 per cent of the world's exposed instances in South Africa, against a global count of 23,286 in the same collection. Both figures stay withheld. The collector should apply the port-concentration test before marking any auto-promoted query VERIFIED, and that change is recorded as a task for the feed rather than as a finding of this report.

## 7.3 The Standing Exposure Panel

---

|                                  |                                                                                                                                                                                                                                 |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MikroTik RouterOS                | 5,627, promoted this week from the catalogue entry; 4,584 on the API port 8728 and 1,043 carrying the sshd product label. The largest population in the panel and the one sitting against a chain with a named attacker address |
| Fortinet FortiGate               | 2,874. Facet resolves cleanly across model variants. The product family behind CVE-2025-25249; a family count, not a count of unpatched builds                                                                                  |
| Citrix Netscaler                 | 104, noting Shodan's lowercase spelling. The population sitting against CVE-2026-19490 and its public exploit                                                                                                                   |
| Microsoft SharePoint on-prem     | 787. Component match. The population sitting against CVE-2026-55040, 24 days overdue                                                                                                                                            |
| SonicWall, all products          | 3,012, summing five product strings; 11 on the SSL-VPN proxy string. It CANNOT be narrowed to the SMA 1000 line that carries four catalogue entries                                                                             |
| Apache Tomcat / Cisco ASA WebVPN | 924 across the Tomcat and Coyote labels; 378 ASA WebVPN on the /+CSCOE+/ path                                                                                                                                                   |
| Exposed RDP and port 445         | 8,173 services on port 3389; 5,384 on port 445, mostly unfingerprinted, so read the second as services on that port rather than identified SMB servers                                                                          |
| WordPress / Langflow / Metabase  | 400, a floor because component detection undercounts; 83; 139                                                                                                                                                                   |
| MLflow / Ray / vCenter           | 99, 68 and 2, carried. The vCenter figure is an external count of a normally internal system                                                                                                                                    |
| ownCloud / Gitea / Artifactory   | 119, 9 and 2, carried. Artifactory sits against four catalogue entries                                                                                                                                                          |
| LiteLLM / ScreenConnect          | WITHHELD, 5,171 and 2,996 returned. See 7.2                                                                                                                                                                                     |

These are point-in-time magnitudes. The collection records that Shodan rescan artefacts have moved individual counts by as much as 73 per cent inside twenty-four hours, so week-on-week movement in these figures is not a finding and none is drawn here.<sup>14</sup> The right use of them is the absolute size of an exposed population sitting against an actively exploited flaw, which this week is 5,627 RouterOS instances against a chain with a published attacker address, 104 NetScaler instances against a public exploit, and 787 SharePoint instances against a chain that is 24 days overdue.

## 8. REGULATORY & POLICY

### 8.1 The Regulator's Register, Read Properly

The correction in Section 1 changes what this report can say about the Information Regulator's publication record, and the corrected picture is this. The enforcement-notices register carries three instruments dated 2026: an enforcement notice against Central Johannesburg TVET College under POPIA section 95 dated 20 May, one against Sibanye Stillwater under PAIA section 77J dated 2 June, and one against the Gauteng Department of Health under PAIA section 77J dated 10 June, the document itself being dated 8 June.<sup>15,16</sup> Nothing dated August or September appears, so the SABS enforcement notice described at the

31 August briefing is still absent from the register two weeks later, and the media statements index carries nothing later than the briefing invitation of 27 August.<sup>59</sup> The KPI therefore moves to fourteen weeks from the June notice. The W37 watch item resolves as that edition said it would if nothing appeared: the pattern is a communications practice rather than a backlog, and this report will now record the count without arguing it each week. Among the proposals the Regulator says it intends to submit to Parliament, described by Werksmans from the briefing, is replacing the grace period with an immediate fine on a finding of non-compliance; no Bill or draft text could be located.<sup>60</sup>

## 8.2 A Supplier's Incident and the 24-Hour Clock

Saturday's two notifications are the first public case of the question this report raised when Joint Communication 5 of 2026 took effect on 1 September: what a regulated financial institution does when the material incident is a supplier's. The template requires initial notification within 24 ordinary hours of the institution classifying an incident as material, with no prescribed threshold, and it states that outsourcing does not transfer the obligation; the Authorities rejected the argument that an administrator's notification could stand in for a fund's.<sup>61</sup> Neither Bidvest Bank's nor EasyEquities' reported notice mentions the FSCA or the Prudential Authority, which is not evidence either way, since those notifications go through the Umoja and Joint Standards portals rather than to customers. The decision each institution had to make was whether potentially affected data at a provider is material before the provider's forensic result is known, and that decision belongs in a written policy before the next one.

Werksmans' cross-border analysis of 9 September puts South Africa's own notification rule in context. Zambia and Zimbabwe require notification within 24 hours, Kenya within 72 hours or 24 for designated critical infrastructure, Rwanda within 48 and Nigeria within 72; South Africa's POPIA section 22 requires notification as soon as reasonably possible with no fixed hour count, but it applies to every security compromise regardless of risk, requires the identity of the intruder if known, and since April 2025 must be filed through the Regulator's mandatory eServices portal.<sup>62</sup> For a South African group with subsidiaries in the region the practical consequence is that the incident response plan needs to be built to the 24-hour floor, since a single incident at a shared provider will trigger the Zambian or Zimbabwean clock, the FSCA clock and the POPIA duty at once.

## 8.3 Fraud: SABRIC's 2025 Figures, Read Twice

Two in-window pieces unpacked SABRIC's 2025 annual crime statistics, published in August. Digital banking crime cost R2.41 billion in 2025, up 29.2 per cent on R1.86 billion in 2024 and more than double 2023, across 110,074 reported incidents at an average of R21,865 each; banking applications carried about 89 per cent of cases and 70.5 per cent of value, internet banking under 9 per cent of cases but 28.6 per cent of value.<sup>63,64</sup> SABRIC's own framing is the one to repeat: the application was the channel through which socially engineered fraud was executed, and the applications were not breached. Vishing was a dominant form of authorised-payment fraud, with once-off payments to newly created beneficiaries, remote-access tools installed under a fraud-prevention pretext, caller-ID spoofing, and reports of isolated cases of cloned voices that could be used to impersonate bank officials or executives.<sup>63</sup> The liability position is illustrated by a National Financial Ombud case in which a customer who surrendered credentials to callers posing as her bank and approved the resulting in-app prompts lost R500,000 and was found not entitled to reimbursement.<sup>63</sup> That case, Bidvest Bank's warning that criminals approach customers while they are

worried, and the actor-published employee bank statements in the Rohloff samples describe the same fraud chain from three positions.

## 8.4 Enforcement, Telemetry and the Quiet Regulators

The Hawks said six Nigerian nationals, alleged members of the Black Axe network, would be handed to the FBI and the United States Secret Service at Cape Town International Airport on the afternoon of Friday 11 September for extradition on charges including wire fraud and money laundering; the report was written ahead of the handover and no confirmation that it took place was located in the window; the men were arrested in South Africa in 2021 and are alleged to have defrauded more than 100 United States women, including pensioners, of more than R100 million through romance scams.<sup>65</sup> First reported by [TechCentral](#), [carrying Reuters](#), on 11 September 2026. Check Point's August telemetry, reported by ITWeb and IT-Online on 11 September, puts South Africa at 2,086 attacks per organisation per week, down 3 per cent year on year and below the global average of 2,422, while Angola, Nigeria and Kenya sit at 5,416, 4,906 and 3,658, and energy and utilities was Africa's most-attacked sector, ahead of financial services and government, across the four African countries Check Point reports.<sup>28,66</sup> That is the one counter-trend figure of the week and it is carried as such: a per-organisation attack rate measures noise as well as intent, and it says nothing about the four confirmations above.

The quiet regulators were checked and were quiet. SARS published no scam alert in the window, the most recent remaining SARS-SCAM-400 of 2 September, a fake High Court summons.<sup>67</sup> Parliament's committee listing for 7 to 10 September carries nothing on cybersecurity, Rand Water, SITA or the Cybercrimes Act, and the Portfolio Committee on Communications and Digital Technologies did not meet.<sup>26</sup> The FIC, ICASA, the NCR and SABRIC's own sites could not be read in this environment and are recorded as unchecked rather than as silent.

## 8.5 Who to Call

Six South African teams are registered with FIRST and remain current in this week's collection: the Cybersecurity Hub for private and public sector organisations, ECS-CSIRT at the State Security Agency for government and military, SA NREN CSIRT for research and education, and the UCT, Standard Bank Group and Vodacom Group teams.<sup>68</sup> An insurer, a bank or a law firm in the position of this week's named organisations has the Cybersecurity Hub as its constituency match. Notifying a CSIRT is not the same as notifying the Information Regulator under POPIA section 22, nor the same as the FSCA and Prudential Authority notification in 8.2; a regulated financial institution whose supplier has lost personal information owes all three.

59. Information Regulator of South Africa, media statements index, most recent entry the media invitation of 27 August 2026, checked 13 September 2026. <https://infoeregulator.org.za/media-statements/>

60. Werksmans Attorneys, The regulator is watching: new enforcement signals for POPIA and PAIA compliance (31 August 2026). <https://werksmans.com/the-regulator-is-watching-new-enforcement-signals-for-popia-and-paia-compliance/>

61. Moonstone, New IT and cyber incident reporting template now in effect, on FSCA and Prudential Authority Joint Communication 5 of 2026 (3 September 2026). <https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>

62. Werksmans Attorneys, When the clock starts ticking: why cross-border data breach response demands more than good intentions (9 September 2026). <https://werksmans.com/when-the-clock-starts-ticking-why-cross-border-data-breach-response-demands-more-than-good-intentions/>

63. Moonstone, How scammers turn your trust against you, unpacking the SABRIC 2025 annual crime statistics (7 September 2026). <https://www.moonstone.co.za/how-scammers-turn-your-trust-against-you/>

64. IOL Business, Banking apps become fraudsters' favourite weapon as South Africans lose R1.7bn (9 September 2026).  
<https://iol.co.za/business/2026-09-09-banking-apps-become-fraudsters-favourite-weapon-as-south-africans-lose-r17bn/>
65. TechCentral / Reuters, South Africa to extradite cyberfraud-gang suspects to US (11 September 2026).  
<https://techcentral.co.za/south-africa-to-extradite-us-cyberfraud-gang-suspects-to-us/286052/>
66. IT-Online, August cyberthreats surge as ransomware nearly doubles (11 September 2026).  
<https://it-online.co.za/2026/09/11/august-cyberthreats-surge-as-ransomware-nearly-doubles/>
67. SARS, Scams and phishing index, most recent entry SARS-SCAM-400 (2 September 2026), checked 13 September 2026.  
<https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
68. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 13 September 2026, six teams.  
<https://www.first.org/members/teams/>

## 9. WEEKLY THREAT HUNT & IOCs

Seven missions. Two P1 cover the actors that named a South African organisation this week, The Gentlemen and LockBit 5.0, both with sourced atomic indicators from the aggregator's per-group feed. Three P1 cover the network-edge and management-plane catalogue entries where a vendor or a named responder confirmed exploitation against internet-facing systems: NetScaler, Cisco FMC and FortiOS, and MikroTik RouterOS. One P2 covers the remote-management and developer-plane additions, N-central, ScreenConnect, Artifactory and GitLab. One P2 covers Adobe Commerce. Chromium and the two Windows zero-days carry no mission and the reason is stated: the browser and operating-system flaws are remediated by the September updates and a fleet restart, and no exploitation detail has been published for the Windows Update Stack flaw. Indicators come from vendor advisories, named responder reporting and the per-group feeds, and the atomic detail is exported to iocs\_w38.csv rather than repeated in full here.<sup>31</sup> No hunt is repeated from a prior week without new justification: the DireWolf mission from W37 is not carried because its incident is now confirmed and its indicators are unchanged, and the two actor missions here are new to this edition.

**TH-2026-W38-01: The Gentlemen: BYOVD, EDR Termination and GPO Deployment****P1 CRITICAL:** SA insurer listed 7 September; FortiGate and stealer-credential access, worming encryptor

**Hypothesis:** A Gentlemen operator has gained access through an unpatched FortiGate appliance or infostealer-harvested credentials, loaded a renamed vulnerable driver to disable endpoint protection from the kernel, moved laterally with PsExec and RDP, staged exfiltration, and is preparing a domain-wide deployment through Group Policy of a Go encryptor that can self-propagate.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1068 (Exploitation for Privilege Escalation), T1211 (BYOVD via CVE-2025-7771), T1562.001 (Impair Defenses), T1021.001/002 (Remote Services: RDP, SMB), T1484.001 (Group Policy Modification), T1567.002 (Exfiltration to Cloud Storage), T1486 (Data Encrypted for Impact).

**IOCs:** Driver ThrottleBlood.sys (renamed ThrottleStop.sys); EDR-termination tools All.exe and Allpatch2.exe; elevation tool PowerRun.exe; ransom note README-GENTLEMEN.txt; six-character random extensions such as .7mtzhh and .ojuopo; AnyDesk installed as a Windows service; exfiltration via WinSCP, Rclone or azcopy. A subset of the aggregator's 85 sample hashes and six Tox identifiers for the group is in iocs\_w38.csv. Primary access CVE-2024-55591 (FortiOS/FortiProxy).

**Data Sources:** Sysmon process and driver-load events, EDR service-control and tamper telemetry, Windows Security logs for GPO changes on the NETLOGON share, RDP and SMB session records, and egress to Wasabi, S3 and Dropbox.

**Detection Guidance:** Alert on a kernel driver loading from a user-writable path, and on any process terminating multiple endpoint-protection services in sequence, because Allpatch2.exe identifies the running EDR dynamically rather than from a fixed list. Alert on a new or modified Group Policy object that writes an executable to many hosts, which is the deployment mechanism. Treat AnyDesk installed as a service on a server as an incident unless it is sanctioned. On the FortiGate side, confirm CVE-2024-55591 is patched, since it is the group's documented primary access route into South African estates.

**TH-2026-W38-02: Citrix NetScaler: RelayState Authentication Bypass****P1 CRITICAL:** public exploit since 2 September, attempts since 3 September, 104 exposed in ZA

**Hypothesis:** An attacker has posted to /cgi/samlauth on a NetScaler Gateway or AAA virtual server so that the decoded RelayState length mints a session as the user anonymous, then used the resulting access as an internal SSRF proxy where the default authorisation action is set to ALLOW. Crashes of the packet engine indicate the length-18 or length-21 path being tried.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1556 (Modify Authentication Process), T1090 (Proxy), T1499 (Endpoint Denial of Service).

**IOCs:** POST to /cgi/samlauth followed by /cgi/setclient?cvpn; an SSL VPN login for the user anonymous in clientless mode with an NSC\_AAAC cookie; unpatched appliances answer a probe with HTTP 500 and internal error 43524, patched ones with HTTP 200 and Malformed Assertion. Bishop Fox's safe checker is public. Fixed builds 14.1-73.32, 13.1-63.21 and 13.1-37.277 FIPS.

**Data Sources:** NetScaler nsvpn and httpaccess logs, authentication and session records, appliance packet-engine restart events, and outbound connections originating from the appliance.

**Detection Guidance:** Alert on any SSL VPN session whose user is anonymous, since every session this exploit creates carries that name and it cannot be forged into a named user. Alert on repeated packet-engine restarts, which are the denial-of-service branch of the same endpoint. Patch both nodes of every HA pair, including the secondary. Check the default authorisation action: shipped as DENY, it limits the bypass to session creation, but where it has been set to ALLOW the attacker gains an internal HTTP proxy. An appliance patched only for August's CVE-2026-8452 is still exposed.

### TH-2026-W38-03: Cisco FMC and FortiOS: Unauthenticated Code Execution on Security Appliances

P1 CRITICAL: Cisco FMC 10.0 exploited since August, three actor clusters; FortiOS PivotC2 since July

**Hypothesis:** An attacker has reached root on a Cisco Secure Firewall Management Center through the CVE-2026-20079 authentication bypass, most likely on an appliance rarely logged into so a stale post-reboot session persists, or has exploited the FortiOS cw\_acd CAPWAP daemon over UDP 5246 to install the PivotC2 remote access tool. On FMC the goal is the configurations of every firewall it manages.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1556 (Modify Authentication Process), T1059 (Command and Scripting Interpreter), T1505.003 (Web Shell), T1552 (Unsecured Credentials), T1602 (Data from Configuration Repository), T1571 (Non-Standard Port).

**IOCs:** Cisco FMC: any request bearing the static cookie CGISESSID=csm\_processes; the log check zgrep for package\_info and license across /var/log/messages, a hit referencing /var/tmp/license.tmp; Talos addresses 89.34.96.56, 208.123.119.215, 104.218.165.253 and hashes for home.jsp, cmd.jar and the Cyclops Blink implant, all in iocs\_w38.csv. FortiOS: SOCRadar C2 46.151.29.58:8443 and 146.103.99.177:8443/9443, the host artefact /tmp/.i.js, and config theft of /data/config/sys\_global.conf.gz. Fixed FMC hot fixes per branch; FortiOS 7.6.4/7.4.9/7.2.12/7.0.18.

**Data Sources:** FMC /var/log/messages and web-server logs, appliance reboot history, Fortinet CAPWAP and local-in policy logs, and netflow to the listed C2 addresses.

**Detection Guidance:** For FMC, treat any request carrying CGISESSID=csm\_processes as exploit traffic and run the vendor log check; because exploitation needs a stale post-reboot session, prioritise appliances that are rarely logged into, which inverts the usual triage. Contact TAC on a positive log hit rather than assuming the hot fix cleaned an existing compromise. For FortiOS, hunt fnsysctl ls -la /tmp/.i.js and sessions to the SOCRadar C2 addresses, and remove fabric from allowaccess or deny UDP 5246 to 5249 as an interim control, since the web interface firewall does not cover the CAPWAP port.

### TH-2026-W38-04: MikroTik RouterOS: SSH Argument Injection to Full Administrator

P1 CRITICAL: named attacker address active since 2 September; 5,627 exposed in ZA

**Hypothesis:** An attacker has reached an internet-facing RouterOS SSH service and used the MikroTrick chain, the CVE-2026-67276 SSH authentication bypass with the CVE-2026-86060 argument injection in the username, to obtain a session with full administrator policy, then created a persistent highly privileged account. This is the largest exposed South African population in the panel and the one with a published attacker address.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1078 (Valid Accounts), T1136 (Create Account), T1556 (Modify Authentication Process), T1499 (Endpoint Denial of Service, via the btest flaw).

**IOCs:** Log lines login failure for user -2 from an address via ssh and user added by ssh:-2; a highly privileged account named ops; source address 82.192.72.4 for successful attacks and 103.102.31.18 for attempts, per CERT Polska. Fixed builds 7.25beta3, 7.24.2, 7.23.4 and 6.49.21; RouterOS marks a device Flagged when it finds selected traces.

**Data Sources:** RouterOS system logs forwarded to a collector, SSH authentication records, the device Flagged status and critical log entry, and account-creation events.

**Detection Guidance:** Alert on the two published log strings and on the creation of any account named ops or any account granted full policy over SSH. Do not treat an unflagged device as clean, because CERT Polska states the marker detects only selected traces. Take RouterOS SSH off the public internet where it does not need to be there, which for most South African deployments is everywhere, and confirm the fixed build rather than relying on the Flagged status.

**TH-2026-W38-05: Management and Developer Plane:  
N-central, ScreenConnect, Artifactory and GitLab****P2 HIGH:** four internet-facing control-plane additions; ScreenConnect worm-like, Artifactory token forgery

**Hypothesis:** An attacker reached a management or developer control-plane service that should not be internet-facing: an N-central server through the pre-auth code injection, a ScreenConnect client turned into a propagation node after a social-engineered install, an Artifactory instance through the anonymous-token to admin-token chain, or a GitLab instance through the unauthenticated commits-API file read.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1078 (Valid Accounts), T1528 (Steal Application Access Token), T1136 (Create Account), T1105 (Ingress Tool Transfer), T1496 (Resource Hijacking), T1005 (Data from Local System).

**IOCs:** N-central: attacker IPs 23.234.100.105 and 23.234.97.68, accounts created by appending .invalid to known N-able email addresses, recon against /remoteControlAction.do; fixed build 2026.3.1.14. ScreenConnect: malicious instance ID 7a4d7d66502d4260, VBScript files 1.vbs to 4.vbs and WindowsServiceHost.vbs as the Run-key persistence script, payloads Themes.exe (wstunnel), SearchIndex.exe (XMRig) and svcdrv64.sys (WinRing0); fixed 26.6.5. Artifactory: unauthenticated POST /access/api/v1/aws/token/, admin actions logged as token:anonymous, account patterns Oxterror and Nxploited; fixed 7.133.11 and the 42018 branches. GitLab: POST to /api/v4/projects/{id}/repository/commits/ with a file.path parameter; fixed 19.3.2/19.2.6/19.1.8. Hashes in iocs\_w38.csv.

**Data Sources:** Reverse proxy and application access logs for each product, token audit logs, ScreenConnect server RunFiles and RanFiles audit entries, container runtime auditing, and egress to mining pools.

**Detection Guidance:** For Artifactory, alert on any admin action logged under token:anonymous, which is the chain's signature, and revoke long-lived tokens as a step separate from the upgrade because the upgrade does not invalidate them. For ScreenConnect, alert on RunFiles or RanFiles entries executing VBScript from Process: Guest and reimagine the host rather than cleaning it. For N-central, alert on account names ending .invalid and on requests to /remoteControlAction.do from outside your management ranges. For GitLab, log and alert on POST requests to the commits API carrying a file.path parameter, which needs no credentials at all.

**TH-2026-W38-06: Adobe Commerce: StyleSmuggler  
Template Injection****P2 HIGH:** unauthenticated 10.0 RCE, exploited from 4 September, three days before the patch

**Hypothesis:** An attacker has exploited CVE-2026-75650 against an internet-facing Adobe Commerce or Magento store, reaching code execution when the store renders a transactional email, and has installed a Rust implant that masquerades as a system process and beacons over UDP 123, or a web shell under the media cache directory. Because execution occurs on email render, a failed delivery does not stop it.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1505.003 (Web Shell), T1053.003 (Scheduled Task/Job: Cron), T1036.005 (Masquerading: Match Legitimate Name), T1571 (Non-Standard Port), T1496 (Resource Hijacking).

**IOCs:** Rust implant masquerading as kworker, fc-cache or chronyd; C2 windwsecurity.run:443 and NTP-mimic endpoints ntp.timesysnc.net:123, time.microsoft.run:123 and 185.157.160.251:123; cron entry running .local/share/gvfsd/gvfsd-user; second operator web shell under pub/media/catalog/product/cache answering only to X-Cache-Token: fced27f6d57702565353ecc11722533b; SHA256 hashes and attacker IPs in iocs\_w38.csv. Fixed by the APSB26-146 hotfix plus key rotation.

**Data Sources:** Magento and web-server access logs, the exception log for the payment-failed email job, outbound UDP 123 flows, cron and process telemetry on the store host, and file-integrity monitoring on pub/media.

**Detection Guidance:** Alert on outbound UDP 123 that is not a single client-mode NTP query to your known time source, since the implant sends bursts of nine server-mode datagrams; a genuine client sends one. Alert on any new file under pub/media/catalog/product/cache with a .php extension. Apply the composer hotfix and, critically, rotate the encryption key and every credential it protects, because Adobe's remediation is not complete without the rotation and a compromised store may already have leaked its keys.

**TH-2026-W38-07: LockBit 5.0: Fixed Encryptor Behaviours on Windows and ESXi****P3 MEDIUM:** SA law firm listed 7 September; family behaviours are stable across LockBit 4.0 and 5.0

**Hypothesis:** A LockBit 5.0 operator is present and has begun the encryption routine on Windows hosts or an ESXi cluster: disabling event tracing, terminating security services against a hashed list, clearing every event log, and encrypting with a randomised sixteen-character extension. The hunt runs on the family's fixed behaviours because 5.0 shares its core with 4.0.

**MITRE ATT&CK:** T1486 (Data Encrypted for Impact), T1562.001 (Impair Defenses: Disable or Modify Tools), T1562.006 (Indicator Blocking, EtwEventWrite patch), T1070.001 (Clear Windows Event Logs), T1489 (Service Stop), T1614.001 (System Location Discovery, the Russian-language geofence).

**IOCs:** Ransom note ReadMeForDecrypt.txt; a randomised sixteen-character file extension; an in-memory patch of EtwEventWrite to 0xC3; termination of services matched against 63 hashed names; EvtClearLog across all logs; on ESXi, targeting of virtual machine configuration files. A subset of the aggregator's thirteen MD5 sample hashes for the group is in iocs\_w38.csv.

**Data Sources:** Sysmon and EDR process telemetry, Windows event log service state, ESXi shell and vpxa logs, and file creation carrying a new uniform sixteen-character extension across a share.

**Detection Guidance:** The extension is the cheapest signal: a directory of files that suddenly share one sixteen-character hexadecimal suffix is the encryption pass in progress. Alert on a process patching or writing to the EtwEventWrite address, and on EvtClearLog issued across multiple logs in sequence. On ESXi, alert on shell access outside a change window, because a single compromised host encrypts every guest. There is no decryptor; the value of the hunt is time before the extension appears fleet-wide.

## 10. STRATEGIC RECOMMENDATIONS

### Technical (SOC / IR)

- 1. Work the seven overdue catalogue additions on Monday 14 September, edge and management plane first.** The seven past due are Citrix NetScaler CVE-2026-19490, Cisco FMC CVE-2026-20079, FortiOS CVE-2025-25249, both MikroTik RouterOS flaws, N-able N-central CVE-2026-86218 and Adobe Commerce CVE-2026-75650; ScreenConnect and GitLab fell due the same day. Fixed versions are in the Section 5 table. Patch both nodes of every NetScaler HA pair, and take Artifactory, N-central and any developer control plane off the public internet while you patch, because none has any business being reachable there.
- 2. Read the catalogue before the vendor page this week.** Three vendor advisories would have under-prioritised a real exploited flaw: Fortinet still reads Known Exploited: No, Citrix does not mention exploitation, and N-able's status page contradicts its own customer notice. Triage from the CISA catalogue date, and use the vendor page for the fixed build while leaving the risk decision to the catalogue.
- 3. Run the appliance-specific compromise checks alongside the patches.** For Cisco FMC, treat CGISSESSID=csm\_processes as exploit traffic and run the zgrep log check; a hit means contacting TAC, because the hot fix stops future exploitation without removing an existing compromise. For MikroTik, hunt the log line user ops added by ssh:-2 and the address 82.192.72.4, and do not trust an unflagged device. For NetScaler, hunt SSL VPN sessions belonging to the user anonymous. These are the published markers and each takes minutes.

**4. Revoke Artifactory tokens and rotate Adobe Commerce keys as tasks separate from patching.** An Artifactory admin token minted through this week's chain survives the upgrade, so enumerate long-lived tokens, revoke anything without a named owner and look for admin actions logged as token:anonymous. An exploited Magento store may have leaked its encryption key, so Adobe's own remediation is the hotfix plus key and credential rotation; the patch alone is not enough.

**5. Restart the browser fleet and confirm the September Windows update.** The two exploited Windows zero-days and the exploited Chrome V8 flaw are one espionage chain, and the remedy for a South African endpoint fleet is the September cumulative update and a Chrome or Edge restart to 153.0.8010.36 or later. Fully patched Windows 11 is outside the kernel exploit's target set; older Windows 10 and Server builds are inside it, so prioritise those.

## Management (CISO / Board)

**1. Ask which of your suppliers would tell you first, and put a number of hours in the contract.** Two financial institutions spent this week telling customers about a provider's breach they could not yet size. The organisations that keep your customer verification, onboarding and screening data are the ones most likely to be the incident you have to disclose, and most have no contractual obligation to notify you on suspicion. Add a stated hour count, an escalation contact and a notify-on-suspicion clause to the next three supplier renewals.

**2. Decide in writing when a supplier's incident becomes material to you.** The FSCA and Prudential Authority 24-hour clock runs from the moment you classify an incident as material, with no prescribed threshold and no relief for outsourced functions. Bidvest Bank and EasyEquities each had to make that call this week. Make yours calmly, in a board-approved policy, before the next provider calls, and remember a single incident at a shared provider can trigger the FSCA clock, POPIA section 22 and a neighbouring country's 24-hour rule at once.

**3. Treat a leak-site listing of your organisation as a communications event as much as a technical one.** The Gentlemen and LockBit 5.0 listed two well-known South African names this week with no data, no sample and no deadline, and in Hollard's case the company answered a journalist rather than the market. Whether or not a claim is real, the moment it is public your customers, brokers and regulators are reading it. Have a holding statement and an escalation path agreed now, because the 22-minute gap between the two listings is how fast this arrives.

**4. Treat conveyancing, verification and other data-rich intermediaries as part of your own risk surface.** A suburban law firm holds identity documents and trust-account records for every property transaction; a verification provider holds the identity data of a bank's entire customer base. The size of the named organisation is a poor guide to the sensitivity of what it holds. Map where your customers' identity data actually sits, including in small suppliers, and price the assurance accordingly.

**5. Read the one good number honestly.** Check Point puts South Africa's per-organisation attack rate down 3 per cent year on year and below the global average, while Angola and Nigeria rose sharply. That is a real data point and it measures attack volume, not outcome. Four South African organisations confirmed breaches this week and two of them were breached through a supplier, so a falling attack rate is not a falling risk, and no assurance argument should lean on it.

## 11. THREAT LEVEL ASSESSMENT

### THREAT LEVEL: HIGH, 21st CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-first consecutive week (6 September to 12 September 2026). Escalation to CRITICAL was considered on the volume of confirmed activity, four victim confirmations and two unresolved claims against major institutions, and rejected on the same criterion applied last week: no systemically important institution went out of service and no national-scale outage occurred. Two of the four confirmations were supplier breaches whose impact on the notifying institutions is not yet known, and both unresolved claims lack any published data, so the evidence supports a busy HIGH rather than an escalation. De-escalation to MEDIUM was rejected on the largest weekly catalogue count this series has recorded, seven of it overdue at publication across the network edge and the management plane, several entries with named active exploitation.

### Rationale

- **Two of the world's three most active ransomware operations named South African organisations in one evening.** The Gentlemen listed the largest private insurer and LockBit 5.0 listed a conveyancing firm, 22 minutes apart, both unresolved and both without published data. Neither is a confirmed breach, and both come from groups with the tooling and the South African access routes to make the claims credible rather than idle.
- **The confirmed damage this week came through suppliers.** Bidvest Bank and EasyEquities each notified customers of a provider breach, Cartrack confirmed an incident reported as ransomware and a regulator notification, and Rohloff Group acknowledged INC Ransom's listing. Four confirmations is the most this series has carried, and the two supplier cases are the ones a peer organisation should study, because the failure was in a party the institution had outsourced to and could not see.
- **The largest catalogue week on record, concentrated on the edge and the management plane.** Fourteen additions, seven overdue at publication, with NetScaler carrying a public exploit, Cisco FMC at 10.0 with three named actor clusters, FortiOS under a named RAT campaign, and MikroTik with a named attacker address against 5,627 exposed South African instances. Three vendor advisories understated the exploitation that the catalogue recorded.
- **The regulator's publication drought is now confirmed as a practice, and a prior-edition error is corrected.** This edition corrects the W37 claim that the register had published nothing since April 2025: it carries three 2026 instruments, the latest dated 10 June. The SABS notice described on 31 August is still not on the register two weeks later, so the fourteen-week count from the June notice stands and the item stops being argued each week.

### Next-Week Watch (W39)

- **Hollard, and whether the claim becomes a confirmation.** Two observations would move it: a Hollard statement acknowledging an intrusion or a POPIA section 22 notification, which would take it from

CLAIMED to CONFIRMED, or The Gentlemen publishing a dataset, which would do the same from the other side. Continued silence from both, as with the same group's Babcock listing, leaves it CLAIMED and is itself informative about how much the group actually holds.

- **Whether Bidvest Bank and EasyEquities were breached through the same provider.** The distinguishing observation is narrow: either institution naming the provider, or a third institution issuing a similar notice, would indicate a shared supplier and a larger event; separate providers would make it a coincidence of timing. Neither has named the firm, and this report will not infer a link until one of those appears.
- **Whether the LiteLLM and ScreenConnect exposure figures resolve under the port test.** The port-concentration test in Section 7.2 explains why both are withheld. The observation that would settle each is a re-derivation that either finds a genuine port cluster, which would make the figure real, or confirms the scatter across hundreds of ports, which marks it a fingerprint or deception artefact. The collector task to apply that test automatically is recorded and is the actual fix.
- **Whether the Cisco FMC and NetScaler exploitation reaches South African victims.** Both flaws have named active exploitation abroad and both products have South African exposure, NetScaler at 104 and FMC unmeasured. The observation to watch is any South African leak-site listing or incident naming an edge-appliance or firewall-management compromise as the entry point, which would connect the exposure panel to a domestic outcome for the first time in several weeks.
- **Rand Water, still open at day seventeen.** The three W37 tests remain: a named actor or family, a statement about personal information, or a return from the Centurion disaster recovery site to the primary. Silence on all three now suggests an investigation still open more than two weeks in, which is itself the finding until one of the three changes.
- **The developer and management-plane exposure, carried from W36 and now resolved as a live problem.** The W36 watch item asked whether exposed developer servers had legs. This week answered it: four of the fourteen catalogue additions land on that estate, Artifactory is under a confirmed in-the-wild token-forgery chain, and the panel figures held steady, so the item stops being a watch and becomes a standing patch priority in Section 5. It is not carried forward as a separate watch.
- **Carryovers held without re-argument.** The Courier Guy, Babcock, Toyota's unnamed SMS provider, the Furniture Bargaining Council exfiltration claim, Implats and Hungry Lion all remain CLAIMED or open with no development. Krybit's South African watch item is closed, and the next South African Krybit listing will be treated as a new observation rather than a resumption.

## 12. OSINT SOURCES CONSULTED

All sources are TLP:CLEAR and publicly accessible, numbered in order of first citation. Every cited URL was retrieved and confirmed to contain the claim attributed to it, on 13 September 2026. **Collection notes.** The feed run completed at 02:05 UTC on 13 September 2026 and passed its integrity check with a clean exit. The victim feed returned 128 records, all tagged ZA; the run log records filter purity 1.0 and the written file records 128 South African records against 128 returned. The catalogue file is catalogVersion 2026.09.11. **Provenance of the machine-read feeds.** Every ransomware.live, NVD and EPSS figure in this report was retrieved from those services' APIs, not from their web pages, and the sources are cited as the endpoints actually called. The distinction matters for this aggregator specifically: its rendered pages and its API have disagreed before, and a figure read from one cannot be cited to the other. Where an endpoint needs a key,

the equivalent public page is named alongside it so a reader without one can still check. **A correction.** This edition corrects the W37 statement that the Information Regulator's enforcement-notices register carried nothing later than 16 April 2025; it carries three 2026 instruments, dated 20 May, 2 June and 10 June, the last being the Gauteng Department of Health notice already used as the KPI anchor. The correction is recorded in Section 1 and applied in Section 8.1; the W37 KPI value and the W37 finding that the SABS notice is absent from the register both stand. **Two figures withheld.** The Shodan collection returned 5,171 LiteLLM and 2,996 ScreenConnect instances in South Africa and marked both VERIFIED on facet purity. Neither is published: their port distributions do not cluster on the products' listening ports, the signature of a fingerprint catching something else, as Section 7.2 sets out. Four catalogue products, GitLab, Adobe Commerce, N-central and Chromium, have no Shodan product label, and Cisco FMC and the SMA 1000 line have none either, so no South African figure is given for any of them. **Environment limitations.** cisa.gov returns an empty body here, so every catalogue date and due date comes from the locally retrieved file. Several primary pages are client-side rendered and were read through a browser or through named secondary reporting: the Cisco, ConnectWise, PaperCut and SonicWall advisory pages, and Rand Water's own media centre, which could not be read at all. **Attribution policy.** Where a story was broken by a publication this report names who broke it, links to them, and summarises only what the intelligence judgement requires. **Single-source disclosure.** Several items rest on one publication because no other account could be found: the Hollard, Bidvest Bank, EasyEquities, Cartrack and Rohloff statements are each carried by MyBroadband; the FSCA template by Moonstone; the cross-border notification analysis by Werksmans. The VSB Attorneys, Hollard and Capricorn listings rest on the aggregator plus the organisations' own websites. **Claims deliberately excluded.** The capricornlogistics.com listing is excluded from every South African count as an Indian company mistagged by the aggregator. No connection is asserted between the Bidvest Bank and EasyEquities supplier incidents. The INC Ransom Netstar listing is dated August 2025 in the local feed, not 2026, and the media claim of 2026 is not carried. No actor or family is attributed to Rand Water. Halcyon's DireWolf and any prior-year victim concentrations are not presented as current.

- ransomware.live, victim record: Hollard Insurance Group, The Gentlemen, discovered 7 September 2026 21:56 UTC. <https://www.ransomware.live/id/SG9sbGFyZCBJbnNlcmFuY2UgR3JvdXBAdGhlZ2VudGxlbWVu>
- ransomware.live, victim record: vsbattorneys.co.za, LockBit 5.0, discovered 7 September 2026 21:34 UTC. <https://www.ransomware.live/id/dnNiYXR0b3JuZXIzLmNvLnphQGxvY2tiaXQ1>
- MyBroadband, South African insurance company allegedly hit by cyberattack (12 September 2026). <https://mybroadband.co.za/news/security/667199-south-african-insurance-company-allegedly-hit-by-cyberattack.html>
- VSB Attorneys Inc, firm website, conveyancing and commercial practice at Meyersdal, Alberton, founded 1988, checked 13 September 2026. <https://www.vsbattorneys.co.za/>
- Hollard, media centre press release index, most recent entry 26 August 2026, checked 13 September 2026. <https://www.hollard.co.za/media-centre/press-releases>
- MyBroadband, South African bank notifies customers of data breach (12 September 2026). <https://mybroadband.co.za/news/security/667328-south-african-bank-notifies-customers-of-data-breach.html>
- MyBroadband, EasyEquities informs customers about possible data breach (12 September 2026). <https://mybroadband.co.za/news/security/667348-easyequities-informs-customers-about-possible-data-breach.html>
- MyBroadband, Top vehicle tracking company in South Africa with 2.2 million subscribers hit by cyberattack (7 September 2026). <https://mybroadband.co.za/news/security/666362-top-vehicle-tracking-company-in-south-africa-with-2-2-million-subscribers-hit-by-cyberattack.html>
- MyBroadband, Large KFC franchise operator in South Africa hit by 536GB data breach (8 September 2026). <https://mybroadband.co.za/news/security/666413-large-kfc-franchise-operator-in-south-africa-hit-by-536gb-data-breach.html>
- CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.11, released 11 September 2026, retrieved 13 September 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Fortinet PSIRT, FG-IR-25-084, heap-based buffer overflow in cw\_acd daemon, last updated 23 February 2026, still reading Known Exploited: No when checked 13 September 2026. <https://fortiguard.fortinet.com/psirt/FG-IR-25-084>
- Citrix, NetScaler ADC and NetScaler Gateway security bulletin for CVE-2026-19489 and CVE-2026-19490, CTX696939 (19 August 2026, unrevised at 13 September 2026). <https://support.citrix.com/external/article/CTX696939/netScaler-adc-and-netScaler-gateway-secu.html>
- Huntress, N-able N-central vulnerability exploitation (updated 6 September 2026). <https://www.huntress.com/blog/n-able-vulnerability-exploitation>
- Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 13 September 2026. <https://www.shodan.io/search?query=country%3AZA>
- Information Regulator of South Africa, enforcement notices register; the 2026 tab carries three instruments dated 20 May, 2 June and 10 June 2026, checked 13 September 2026. <https://inforegulator.org.za/enforcement-notices/>

16. Information Regulator of South Africa, Gauteng Department of Health enforcement notice dated 8 June 2026 and listed 10 June 2026, the anchor for the weeks-since-publication count.  
<https://infoeregulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>
17. ransomware.live API, SA victim records, GET /v2/countryvictims/ZA, 128 records all tagged ZA, retrieved 02:00 UTC 13 September 2026.  
<https://api.ransomware.live/v2/countryvictims/ZA>
18. Cisco Talos, Ongoing exploitation of Cisco Secure Firewall Management Center (9 September 2026).  
<https://blog.talosintelligence.com/fmc-ongoing-exploitation/>
19. SOCRadar, CVE-2025-25249 exploited in the wild: PivotC2 RAT campaign against FortiGate (8 September 2026).  
<https://socradar.io/blog/cve-2025-25249-pivotc2-fortigate-rat/>
20. ransomware.live API PRO, group index GET /groups: The Gentlemen, 838 victims across 86 countries, retrieved 13 September 2026 (public page: ransomware.live/group/thegentlemen). <https://api-pro.ransomware.live/groups>
21. Blackpoint Cyber, Threat profile: The Gentlemen ransomware (3 August 2026).  
<https://blackpointcyber.com/threat-profile/gentlemen-ransomware/>
22. Karooooo Limited, JSE SENS announcements index, most recent entry 28 July 2026, checked 13 September 2026.  
<https://karooooo.com/jse-sens-announcements/>
23. ransomware.live API PRO, group index GET /groups: DireWolf, 135 victims across 37 countries, retrieved 13 September 2026 (public page: ransomware.live/group/direwolf). <https://api-pro.ransomware.live/groups>
24. ransomware.live, search API record: capricornlogistics.com, Krybit, discovered 12 September 2026, country field ZA against a description reading Indian, Mumbai. <https://api.ransomware.live/v2/searchvictims/capricorn>
25. Capricorn Logistics, company website, registered address Kondivita Road, Andheri East, Mumbai, telephone +91 22, checked 13 September 2026. <https://www.capricornlogistics.com/>
26. Parliamentary Monitoring Group, committee meetings index, complete listing for 7 to 10 September 2026, checked 13 September 2026. <https://pmg.org.za/committee-meetings/?page=1>
27. Industrial Cyber, reporting Check Point Research Q1 2026 ransomware figures: Qilin, LockBit and The Gentlemen expand influence (12 May 2026). <https://industrialcyber.co/ransomware/ransomware-sector-reconsolidating-as-qilin-lockbit-and-the-gentlemen-expand-influence-in-q1-2026/>
28. ITWeb, Check Point red flags heightened attacks on Africa's energy and utilities sectors (11 September 2026). <https://www.itweb.co.za/article/check-point-red-flags-heightened-attacks-on-africas-energy-and-utilities-sectors/Pero3MZ36XdqQb6m>
29. Red Piranha, The Gentlemen ransomware analysis (updated 11 June 2026).  
<https://redpiranha.net/news/the-gentlemen-ransomware-analysis>
30. Microsoft Threat Intelligence, The Gentlemen ransomware: dissecting a self-propagating Go encryptor (28 May 2026).  
<https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/>
31. ransomware.live API PRO, per-group endpoints GET /iocs/{group}, /yara/{group} and /ransomnotes/{group}, retrieved 13 September 2026 (key required; the public group pages carry the same sets). <https://api-pro.ransomware.live/iocs/thegentlemen>
32. Trend Micro, New LockBit 5.0 targets Windows, Linux, ESXi (25 September 2025).  
[https://www.trendmicro.com/es\\_mx/research/25/i/lockbit-5-targets-windows-linux-esxi.html](https://www.trendmicro.com/es_mx/research/25/i/lockbit-5-targets-windows-linux-esxi.html)
33. ransomware.live API PRO, group index GET /groups: LockBit 5.0, 359 victims across 68 countries, last seen 10 September 2026, retrieved 13 September 2026 (public page: ransomware.live/group/lockbit5). <https://api-pro.ransomware.live/groups>
34. SOCRadar, Dark web profile: Krybit ransomware (13 July 2026). <https://socradar.io/blog/dark-web-profile-krybit-ransomware/>
35. NVD API, CVSS base scores with scoring source, GET /rest/json/cves/2.0?cveId=, 53 CVEs resolved, retrieved 13 September 2026.  
<https://services.nvd.nist.gov/rest/json/cves/2.0>
36. BleepingComputer, Hackers target critical Citrix NetScaler auth bypass in attacks (4 September 2026).  
<https://www.bleepingcomputer.com/news/security/hackers-target-critical-citrix-netscaler-auth-bypass-in-attacks/>
37. Bishop Fox, Mind the config: detecting and weaponizing NetScaler CVE-2026-19490 (10 September 2026).  
<https://bishopfox.com/blog/mind-the-config-detecting-and-weaponizing-netscaler-cve-2026-19490>
38. Cisco, Security advisory cisco-sa-onprem-fmc-authbypass-5JpP45V2, version 2.5 updated to record active exploitation (9 September 2026).  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JpP45V2>
39. VulnCheck, Cisco FMC authentication bypass CVE-2026-20079 analysis (26 March 2026).  
<https://www.vulncheck.com/blog/cisco-fmc-auth-bypass-cve-2026-20079>
40. CERT Polska, Vulnerabilities in MikroTik RouterOS actively exploited (5 September 2026).  
<https://cert.pl/en/posts/2026/09/vulnerabilities-in-mikrotik-routeros-actively-exploited/>
41. MikroTik, September 2026 vulnerability notice, fixed in RouterOS 7.24.2, 7.23.4 and 6.49.21 (3 September 2026).  
<https://mikrotik.com/supportsec/september-2026-vulnerability/>
42. N-able, N-central 2026.3 Hotfix 4 for CVE-2026-86218, build 2026.3.1.14 (6 September 2026).  
<https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/>
43. ConnectWise, ScreenConnect 26.6.5 security patch bulletin (8 September 2026).  
<https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin>
44. Huntress, Rogue ScreenConnect installations across unrelated hosts suggest worm-like activity (updated 9 September 2026).  
<https://www.huntress.com/blog/rogue-screenconnect-installations>
45. Adobe, Security update available for Adobe Commerce, APSB26-146 (7 September 2026).  
<https://helpx.adobe.com/security/products/magento/apsb26-146.html>
46. Sansec, StyleSmuggler: unauthenticated Magento zero-day exploited in the wild (5 September 2026, updated 11 September 2026).  
<https://sansec.io/research/stylesheet-smuggler-0day>
47. Wiz Research, Artifactory under attack: in-the-wild exploitation of CVE-2026-42016 and CVE-2026-42018 (10 September 2026).  
<https://www.wiz.io/blog/artifactory-under-attack-in-the-wild-exploitation-of-cve-2026-42016-cve-2026-42018>
48. JFrog, Security advisories index, entries for CVE-2026-42016 (27 July 2026) and CVE-2026-42018 (12 August 2026).  
<https://docs.jfrog.com/releases/docs/jfrog-security-advisories>
49. GitLab, Critical patch release 19.3.2, 19.2.6 and 19.1.8 (10 September 2026).  
<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/>
50. watchtower, Rapid reaction: GitLab critical path traversal CVE-2026-85706 (11 September 2026).  
<https://watchtower.com/resources/rapid-reaction-gitlab-critical-path-traversal-vulnerability-cve-2026-85706/>
51. Tenable, Microsoft's September 2026 Patch Tuesday addresses 964 CVEs, CVE-2026-81963 and CVE-2026-85880 (8 September 2026).  
<https://www.tenable.com/blog/microsofts-september-2026-patch-tuesday-addresses-964-cves-cve-2026-81963-cve-2026-85880>
52. Google, Chrome Releases: stable channel update for desktop, 153.0.8010.36 and .37 (8 September 2026).  
[https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop\\_0808145027.html](https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html)

53. Volexity, Mind the patch gap: multiple Chinese threat actors chain zero-day exploits in Chrome and Windows (9 September 2026). <https://www.volexity.com/blog/2026/09/09/mind-the-patch-gap-multiple-chinese-threat-actors-chain-0-day-exploits-in-chrome-windows/>
54. Proofpoint, Once in a BlueMoon: multiple state-aligned threat actors rapidly adopt a novel exploit (9 September 2026). <https://www.proofpoint.com/us/blog/threat-insight/once-blue-moon-multiple-state-aligned-threat-actors-rapidly-adopt-novel-exploit>
55. PaperCut, Security bulletin of 27 August 2026, updated 10 September 2026 with security maintenance releases 26.0.5, 25.0.13 and 24.1.10. <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>
56. GreyNoise, Agents gone wild: an AI-orchestrated global campaign against PaperCut NG/MF (9 September 2026). <https://www.greynoise.io/blog/ai-orchestrated-campaign-against-papercut-ng-mf>
57. Blackpoint Cyber, Death by a thousand PaperCuts: AI-driven exploitation at scale (9 September 2026). <https://blackpointcyber.com/blog/death-by-a-thousand-papercuts-ai-driven-exploitation-at-scale/>
58. FIRST EPSS API, GET /data/v1/epss?cve=, 53 CVEs scored, retrieved 13 September 2026. <https://api.first.org/data/v1/epss>
59. Information Regulator of South Africa, media statements index, most recent entry the media invitation of 27 August 2026, checked 13 September 2026. <https://infoeregulator.org.za/media-statements/>
60. Werksmans Attorneys, The regulator is watching: new enforcement signals for POPIA and PAIA compliance (31 August 2026). <https://werksmans.com/the-regulator-is-watching-new-enforcement-signals-for-popia-and-paia-compliance/>
61. Moonstone, New IT and cyber incident reporting template now in effect, on FSCA and Prudential Authority Joint Communication 5 of 2026 (3 September 2026). <https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>
62. Werksmans Attorneys, When the clock starts ticking: why cross-border data breach response demands more than good intentions (9 September 2026). <https://werksmans.com/when-the-clock-starts-ticking-why-cross-border-data-breach-response-demands-more-than-good-intentions/>
63. Moonstone, How scammers turn your trust against you, unpacking the SABRIC 2025 annual crime statistics (7 September 2026). <https://www.moonstone.co.za/how-scammers-turn-your-trust-against-you/>
64. IOL Business, Banking apps become fraudsters' favourite weapon as South Africans lose R1.7bn (9 September 2026). <https://iol.co.za/business/2026-09-09-banking-apps-become-fraudsters-favourite-weapon-as-south-africans-lose-r17bn/>
65. TechCentral / Reuters, South Africa to extradite cyberfraud-gang suspects to US (11 September 2026). <https://techcentral.co.za/south-africa-to-extradite-us-cyberfraud-gang-suspects-to-us/286052/>
66. IT-Online, August cyberthreats surge as ransomware nearly doubles (11 September 2026). <https://it-online.co.za/2026/09/11/august-cyberthreats-surge-as-ransomware-nearly-doubles/>
67. SARS, Scams and phishing index, most recent entry SARS-SCAM-400 (2 September 2026), checked 13 September 2026. <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
68. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 13 September 2026, six teams. <https://www.first.org/members/teams/>

**TLP:CLEAR.** Distributable without restriction. Compiled from open sources and from feeds retrieved under the compiler's own credentials, and identifies no South African organisation as running a specific exposed system.